Theorie des Kreiskörpers und die Zerlegung von Primteilern eines beliebigen algebraischen Zahlkörpers in einem durch ein irreduzibles Binom definierten Oberkörper.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

Hohen Philosophischen Fakultät

der Philipps-Universität zu Marburg a. d. Lahn

vorgelegt von

Friedrich Oppenheimer
aus Michelstadt i. Odw.

Marburg a. d. Lahn
R. Friedrich's Universitäts-Buchdruckerei (Inhaber Karl Gleiser).
1929.

Als Dissertation angenommen am 17. Juli 1929.
Referent: Geh. Reg.-Rat Professor Dr. K. Hensel.
Tag der mündlichen Prüfung 17. Juli 1929.

Gedruckt mit Genehmigung der Fakultät.

R. UNIV.
BIBLIOTHEEK
LEIDEN

Meinen lieben Eltern

in Verehrung und Dankbarkeit!

Inhaltsübersicht.

Seite

Einleitung 1

I. Teil. Zur Theorie des Kreiskörpers 4

Abschnitt I: Die Zerlegung der rationalen Primzahlen im Körper $\mathfrak{K}_n$ der n-ten Einheitswurzeln 4

§ 1: Der Fall $(p, n) = 1$ 5

§ 2: Verallgemeinerung auf den Fall eines beliebigen algebraischen Zahlkörpers als Grundkörper 6

§ 3: Die Zerlegung der Primzahl p im Falle $n = p^h$ 8

§ 4: Die Zerlegung von p im Falle $n = p^h n'$, $(p, n') = 1$ . . . 10

Abschnitt II: Der Zusammenhang der Kummerschen Theorie der idealen Primfaktoren von p in $\mathfrak{K}_n$ mit der $\mathfrak{p}$-adischen Primteilertheorie 14

§ 1: Grundzüge der Kummerschen Theorie 14

§ 2: Übergang zu den p-adischen Zahlen 19

§ 3: Die Zerlegung von $F_n(x)$ in $K(p)$ 22

§ 4: Eindeutigkeit der Kummerschen Zuordnungen 25

§ 5: Herleitung der Kummerschen Zuordnungen aus der Zerlegung von $F_n(x)$ in $K(p)$ 27

§ 6: Verallgemeinerung der „Kummerschen Kongruenzbedingungen für die Teilbarkeit einer ganzen Zahl aus $\mathfrak{K}_n$ durch eine Primteilerpotenz“ auf den Fall eines beliebigen algebraischen Zahlkörpers 30

II. Teil. Zerlegung von Primteilern eines algebraischen Zahlkörpers in einem durch ein beliebiges irreduzibles Binom definierten Oberkörper 32

§ 1: Einleitende Hilfsbetrachtungen 32

§ 2: Die Zerlegung von $\mathfrak{p}$ in $k(x)$. (Im Falle $(p, n) = 1$) . . . 35

§ 3: Spezialfälle 39

Anhang. Über algebraische Auflösbarkeit Galoisscher Polynome . . . 43

Einleitung.

Durch die von Herrn Hensel gegebene Theorie der algebraischen Zahlen[1]) wird das rein arithmetische Problem der Zerlegung einer rationalen Primzahl p in Primteiler oder Primideale irgendeines algebraischen Zahlkörpers k auf das algebraische Problem der Zerlegung des den Körper k definierenden irreduziblen Polynoms $F(x)$ aus $K(1)$ (Körper der rationalen Zahlen) in irreduzible Faktoren des Körpers $K(p)$ der rationalen p-adischen Zahlen zurückgeführt. Es wird nämlich gezeigt, daß p in ebensoviele Primteiler des Körpers k zerfällt, wie $F(x)$ in $K(p)$ irreduzible Faktoren $f_i(x)$ besitzt. Ist $\mathfrak{p}_i$ der $f_i(x)$ zugeordnete Primteiler des p, so gilt für den Grad f_i und die Ordnung e_i von $\mathfrak{p}_i$ die Relation $e_i f_i = \mu_i$, wenn μ_i der Grad von $f_i(x)$ ist. Ganz das Entsprechende gilt für die Zerlegung irgendeines Primteilers $\mathfrak{p}$ f-ten Grades und e-ter Ordnung eines beliebigen algebraischen Zahlkörpers k in einem durch eine Wurzel x eines irreduziblen Polynoms $F(x)$ aus k definierten Oberkörper $k(x)$ von k. Es gilt auch hier, daß $\mathfrak{p}$ in $k(x)$ so viele Primteiler $\mathfrak{P}_i$ besitzt, wie $F(x)$ irreduzible Faktoren $f_i(x)$ im Körper $k(\mathfrak{p})$, dem Bereiche aller zu k gehörigen $\mathfrak{p}$-adischen algebraischen Zahlen, enthält. Für Relativgrad f_i' und Relativordnung e_i' von $\mathfrak{P}_i$ gilt die entsprechende Relation wie oben, nämlich $e_i' f_i' = \mu_i$, wenn

1) Als grundlegend für diese Theorie seien folgende Schriften des Herrn Hensel, die wir im folgenden mit den in Klammern beigefügten Abkürzungen zitieren, genannt.

1. „Theorie der algebraischen Zahlen", Teubner, Leipzig 1908 (A. Z.).
2. „Über die zu einer algebraischen Gleichung gehörigen Auflösungskörper", Crelles Journal, Bd. 136 (Cr. J. 136).
3. „Eine neue Theorie der algebraischen Zahlen". Mathem. Zeitschrift, Bd. 2 (M. Z. 2).
4. „Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers". Crelles Journal, Bd. 146 (Cr. J. 146).

μ_i der Grad des zugeordneten Polynoms $f_i(x)$ in $k(\mathfrak{p})$ ist. Ich bemerke schließlich noch, daß der Grad von $\mathfrak{P}_i$ gleich ff_i' und die Ordnung gleich ee_i' ist.

Wir wollen im ersten Teil dieser Abhandlung die Henselsche Methode zur Untersuchung der Zerlegungsgesetze der rationalen Primzahlen im Körper $\mathfrak{K}_n$ der n-ten Einheitswurzeln, welche zum ersten Male von E. Kummer in seiner Abhandlung „Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist“ in den „Abhandlungen der Kgl. Akademie der Wissenschaften zu Berlin“ 1856 (zitiert mit B. Ak.) aufgestellt wurden, anwenden und den Zusammenhang mit Kummers Theorie darstellen. Es wird sich zeigen, daß durch eine geeignete Erweiterung der Kummerschen Ideen die Zerlegung der den Körper $\mathfrak{K}_n$ definierenden Funktion in irreduzible Faktoren des Körpers $K(p)$ hergestellt werden kann und daß umgekehrt aus dieser Zerlegung die der Kummerschen Theorie zugrunde liegenden und zur Definition der idealen Primfaktoren des p führenden Sätze auf p-adischem Wege erschlossen werden können. Außerdem werden wir auf p-adischem Wege sehen, daß die von Kummer für die Teilbarkeit einer ganzen Zahl aus $\mathfrak{K}_n$ durch eine beliebige ganze Potenz irgendeines Primteilers von $\mathfrak{K}_n$ angegebenen Kongruenzbedingungen nur ein Spezialfall eines allgemeinen, für beliebige algebraische Zahlkörper geltenden Theoremes sind.

Im zweiten Teil werden wir die Zerlegung eines Primteilers $\mathfrak{p}$ irgendeines algebraischen Zahlkörpers k in einem durch ein beliebiges irreduzibles Binom $x^n - A$ aus k definierten Oberkörper $k(x)$ über k behandeln. Wir werden uns dabei aus später angegebenen Gründen auf den Fall beschränken, daß die zu $\mathfrak{p}$ gehörige rationale Primzahl p zu n teilerfremd ist. Es wird sich ergeben, daß dieses Problem vollständig auf die Betrachtung reiner Eisensteinscher und gewisser Kreisteilungsgleichungen zurückgeführt werden kann. Den anderen Fall, daß p Teiler von n ist, möchte ich mir für eine spätere Arbeit vorbehalten[1]).

1) Für den speziellen Fall, daß n eine Primzahl ist, vergl. man folgende Abhandlungen: K. Hensel: „Über die Zerlegung der Primteiler in relativzyklischen Körpern, nebst einer Anwendung auf die Kummerschen Körper“. (Crelles Journal Bd 151). K. Hensel: „Die Zerlegung der Primteiler eines be-

Im Anhang zur vorliegenden Arbeit erhalten wir aus der Theorie der p-adischen Zahlen ein hinreichendes Kriterium für die algebraische Auflösbarkeit Galoisscher Polynome und einen einfachen Beweis zu dem von Herrn Hilbert aufgestellten Satz, daß ein Galoisscher Zahlkörper stets über den zu seinen Primidealen gehörigen Zerlegungskörpern algebraisch auflösbar ist[1]).

---

liebigen Zahlkörpers in einem auflösbaren Oberkörper" (Crelles Journal Bd. 151). T. Rella: „Bemerkungen zu Herrn Hensels Arbeit ‚Die Zerlegung der Primteiler eines beliebigen Zahlkörpers in einem auflösbaren Oberkörper'". (Crelles Journal Bd. 153). G. E. Wahlin: „The Equation $x^l - A = 0$ (p)" (Crelles Journal Bd. 145).

Schließlich sei noch auf die Dissertation von Herrn W. Theis „Die Zerlegung der reellen Primzahl p in ihre idealen Primfaktoren im Bereiche $R(x, \text{ mod } x^{q^k} - A)$", Marburg Phil. Diss. 1922 hingewiesen, in der dieses Problem für den Fall, daß n Primzahlpotenz und $K(1)$ der Grundkörper ist, vollständig behandelt wird.

1) D. Hilbert, „Die Theorie der algebraischen Zahlkörper". Jahresber. d. deutsch. Math. Ver. Bd. 4 § 49 Satz 82.

I. Teil.

Zur Theorie des Kreiskörpers.

Abschnitt I.

Die Zerlegung der rationalen Primzahlen im Körper $\Re_n$ der n-ten Einheitswurzeln.

Es sei n eine beliebige ganze rationale Zahl ($n > 2$) und $\Re_n$ der Körper der n-ten Einheitswurzeln. Er entsteht durch Adjunktion einer Wurzel ω der in $K(1)$ irreduziblen Gleichung $\varphi(n)$-ten Grades

1) $$F_n(x) = 0,$$

der alle und nur die primitiven Wurzeln der Gleichung

2) $$x^n - 1 = 0$$

genügen, zu $K(1)$ und ist ein Galoisscher Körper $\varphi(n)$-ten Grades.

Bevor ich mit der eigentlichen Untersuchung beginne, seien zwei von Herrn Hensel herrührende Sätze erwähnt, die ich im folgenden benötige.

Hilfssatz 1. Paßt eine Einheitswurzel η zum Exponenten f_0 (bezüglich der Primzahl p), d. h. ist f_0 der kleinste Exponent, für den $\eta^{p^{f_0}} = \eta$, so genügt η einer irreduziblen Gleichung vom Grade f_0 in $K(p)$. Die f_0 Zahlen η, η^p, ... $\eta^{p^{f_0-1}}$ sind sämtliche (konjugierte) Wurzeln dieser Gleichung (A. Z. S. 191 f.).

Hilfssatz 2. Sei k ein beliebiger algebraischer Zahlkörper, $\mathfrak{p}$ ein Primteiler f-ten Grades und e-ter Ordnung von k und p die zugehörige rationale Primzahl, so enthält der Körper $k(\mathfrak{p})$ alle und nur die $p^\nu(p^f - 1)$-ten Einheitswurzeln, wobei ν eine von der Natur des Körpers k abhängige ganze rationale Zahl $\geqq 0$ bedeutet. (Cr. J. 146, S. 212/13).

Zwei Zeichen will ich hier noch zufügen: (a, b) soll wie üblich den größten gemeinsamen Teiler von a und b, und a/b a Teiler von b bedeuten.

Bei der Zerlegung der rationalen Primzahlen p in $\mathfrak{R}_n$ sind die beiden Fälle $(p, n) = 1$ und p/n zu unterscheiden.

§ 1. Der Fall $(p, n) = 1$.

Es sei $(p, n) = 1$ und t der Exponent, zu dem die Primzahl p mod n gehört, d. h. der kleinste Exponent, für den $p^t \equiv 1 \bmod n$ ist, dann ist t auch der Exponent, zu dem die primitive n-te Einheitswurzel ω paßt (bezügl. p). Denn aus $\omega^{p^t} = \omega$ oder $\omega^{p^t-1} = 1$ folgt ja, daß $p^t \equiv 1 \bmod n$ sein muß, t sollte aber gerade der kleinste Exponent sein, für den letztere Kongruenz richtig ist. Sei nun

$$F_n(x) = f_1(x) f_2(x) \ldots f_s(x) \quad (p) \tag{3}$$

die Zerlegung von $F_n(x)$ in irreduzible Faktoren in $K(p)$. Da $F_n(x)$ und somit auch jeder der Faktoren $f_i(x)$ in 3) nur primitive n-te Einheitswurzeln, also nur zum Exponenten t passende Einheitswurzeln enthält, so ist nach Hilfssatz 1 jeder der Faktoren $f_i(x)$ vom Grade t. Für die Anzahl s dieser Faktoren ergibt sich somit

$$s = \frac{\varphi(n)}{t}. \tag{4}$$

Jedem der Faktoren $f_i(x)$ ordnen wir einen Primteiler $\mathfrak{p}_i$ von p zu, für dessen Grad f_i und Ordnung e_i die Relation

$$e_i f_i = t \tag{5}$$

gilt (vgl. Einleitung), d. h. es ist f_i/t. Nach Hilfssatz 2 muß aber wegen $(p, n) = 1$ $n/(p^{f_i} - 1)$, also umgekehrt t/f_i sein. Daraus folgt

$$f_i = t, \quad e_i = 1. \tag{6}$$

Die Primteiler $\mathfrak{p}_i$ sind also keine Verzweigungsteiler[1]), die Körperdiskriminante enthält somit p nicht, und p ist selbst Primelement für den Bereich jedes Primteilers $\mathfrak{p}_i$. Somit gilt:

Satz 1. Sei p eine zu n teilerfremde Primzahl und t der Exponent, zu dem p mod n gehört, so zerfällt p in $s = \frac{\varphi(n)}{t}$ ver-

1) Verzweigungsteiler sind Primteiler, deren Ordnung > 1 ist. Nur diese sind nach einem allgemeinen Theorem in der Körperdiskriminante enthalten.

schiedene Primteiler t-ten Grades und 1-ter Ordnung in $\mathfrak{R}_n$. Diese sind keine Verzweigungsteiler, und die Diskriminante von $\mathfrak{R}_n$ enthält p nicht.

Sei jetzt $\mathfrak{p}$ irgendeiner der s Primteiler des p, $f(x)$ das zugehörige Polynom in $K(p)$ und $\bar{\omega}$ eine Wurzel der Gleichung

7) $$f(x) = 0 \quad (p).$$

Da die Diskriminante von $x^n - 1$ wegen $(p, n) = 1$ bekanntlich p nicht enthält, so enthält diejenige von $f(x)$, weil $f(x)/F_n(x)/(x^n - 1)$ ist, p ebenfalls nicht. Somit bilden die t Zahlen

8) $$1, \bar{\omega}, \bar{\omega}^2, \ldots \bar{\omega}^{t-1}$$

ein Fundamentalsystem für den Bereich von $\mathfrak{p}$[1]), d. h. jede ganze Zahl γ des Körpers $\mathfrak{R}_n$ läßt sich eindeutig in der Form

9) $$\gamma = c_0 + c_1\bar{\omega} + c_2\bar{\omega}^2 + \ldots + c_{t-1}\bar{\omega}^{t-1} \quad (\mathfrak{p})$$

mit ganzzahligen Koeffizienten c_i aus $K(p)$ darstellen. Wir erhalten:

Satz 2. Unter den Voraussetzungen von Satz 1 bilden die Zahlen $1, \bar{\omega}, \bar{\omega}^2, \ldots \bar{\omega}^{t-1}$ ein Fundamentalsystem für den Bereich des Primteilers $\mathfrak{p}$ von p, wobei $\bar{\omega}$ eine Wurzel des zu $\mathfrak{p}$ gehörigen Polynoms in $\mathfrak{R}_n(\mathfrak{p})$ bedeutet.

§ 2. Verallgemeinerung auf den Fall eines beliebigen algebraischen Zahlkörpers als Grundkörper.

Die Henselsche Theorie gestattet nun auch folgende allgemeinere Frage in sehr einfacher Weise zu beantworten:

Gegeben sei ein algebraischer Zahlkörper k, $\mathfrak{p}$ sei ein beliebiger Primteiler f-ten Grades und e-ter Ordnung von k, dessen zugehörige rationale Primzahl p zu n teilerfremd ist. Wie zerfällt $\mathfrak{p}$ in dem durch eine primitive Wurzel ω der Gleichung $x^n - 1 = 0$ definierten Oberkörper $\mathfrak{R}$ von k?

Ich benutze zur Lösung dieser Frage folgenden Hilfssatz, der eine Verallgemeinerung des Hilfssatzes 1 darstellt.

Hilfssatz 3: Sei ω eine primitive n-te Einheitswurzel, $\mathfrak{p}$ ein Primteiler f-ten Grades und e-ter Ordnung von k, $(p, n) = 1$ und f' der Exponent, zu dem p^f mod n gehört, so genügt ω in $k(\mathfrak{p})$ einer irreduziblen Gleichung vom Grade f'.

---

1) A. Z. S. 215/16.

Dieser Satz wurde von Herrn Tonio Rella in der auf S. 3 zitierten Arbeit unter der Annahme, daß n eine Primzahl sei, bewiesen. Doch bleibt alles dort Gesagte richtig, wenn diese Annahme fallen gelassen, n als beliebige ganze rationale Zahl und $(p, n) = 1$ angenommen wird. Dieser Hinweis möge für den Beweis des Satzes genügen.

Ist $n/(p^f - 1)$, also $f' = 1$, so ist dieser Satz trivial, da ja dann nach Hilfssatz 2 $k(\mathfrak{p})$ die primitiven n-ten Einheitswurzeln enthält. Man erkennt ferner, daß im Falle $k = K(1)$, also $\mathfrak{p} = p$ und $f = 1$, dieser Satz in Hilfssatz 1 übergeht.

Sei

10) $$F_n^{(k)}(x) = 0$$

die irreduzible Gleichung, der ω in k genügt und m der Grad von $F_n^{(k)}(x)$, so folgt aus Hilfssatz 3, weil $F_n^{(k)}(x)$ nur primitive n-te Einheitswurzeln enthält, daß $F_n^{(k)}(x)$ in $k(\mathfrak{p})$ in $\frac{m}{f'}$ irreduzible Faktoren f'-ten Grades zerfällt, und somit $\mathfrak{p}$ ebenfalls in $\frac{m}{f'}$ Primteiler $\mathfrak{P}_i$ des Körpers $\mathfrak{K} = k(\omega)$, für deren Relativgrad f_i' und Relativordnung e_i' nach dem in der Einleitung Gesagten die Beziehung

11) $$e_i' f_i' = f'$$

gilt. Nun enthält $\mathfrak{K}(\mathfrak{P}_i)$, weil ff_i' der Grad von $\mathfrak{P}_i$ ist, nach Hilfssatz 2 (von evtl. p^ν-ten Einheitswurzeln abgesehen) nur die $(p^{f f_i'} - 1)$-ten Einheitswurzeln. Andererseits sind nach dem oben erwähnten Beweise des Herrn Rella auch die $(p^{\beta'} - 1)$-ten Einheitswurzeln in $\mathfrak{K}(\mathfrak{P}_i)$ enthalten. Es muß daher f'/f_i' sein, woraus in Verbindung mit 11) folgt: $f_i = f'$, $e_i' = 1$.

Somit ergibt sich:

Satz 3: Genügt die primitive n-te Einheitswurzel ω in dem Körper k einer irreduziblen Gleichung m-ten Grades, ist ferner $\mathfrak{p}$ ein Primteiler f-ten Grades und e-ter Ordnung von p in k, $(p, n) = 1$ nnd f' der Exponent, zu dem p^f mod n gehört, so zerfällt $\mathfrak{p}$ in $k(\omega)$ in $\frac{m}{f'}$ verschiedene Primteiler vom Relativgrade f' und der Relativordnung 1[1]).

1) Ueber die entsprechende Frage im Falle eines Körpers der Charakteristik p als Grundkörper und den Zusammenhang mit der Theorie der $\mathfrak{p}$-adischen Zahlen vgl. man die Abhandlung von Herrn H. Rauter: „Höhere Kreiskörper“ (Crelles Journal Bd. 159).

§ 3. Die Zerlegung der Primzahl p im Falle $n = p^h$.

Der Körper $\Re_{p^h}$ der p^h-ten Einheitswurzeln ist durch die in $K(1)$ irreduzible Gleichung

12) $$F_{p^h}(x) = \frac{x^{p^h} - 1}{x^{p^{h-1}} - 1} = x^{p^{h-1}(p-1)} + x^{p^{h-1}(p-2)} + \ldots + x^{p^{h-1}} + 1 = 0$$

$\varphi(p^h) = p^{h-1}(p-1)$-ten Grades, der alle und nur die primitiven p^h-ten Einheitswurzeln genügen, definiert. Sie ist auch in $K(p)$ irreduzibel. Denn durch die Substitution $x = 1 - y$ geht 12) in eine Eisensteinsche Gleichung

13) $$G(y) = F_{p^h}(1-y) = y^{p^{h-1}(p-1)} \mp \ldots + p = 0$$

mit dem konstanten Gliede p über, und ist daher in $K(p)$ irreduzibel. (A. Z. S. 76). p besitzt daher nur einen einzigen Primteiler $\mathfrak{p}$ in $\Re_{p^h}$. Bezeichnet ζ eine Wurzel von $F_{p^h}(x) = 0$ (p) und wird $\pi = 1 - \zeta$ gesetzt, so folgt aus $G(y) = F_{p^h}(1-y)$, daß π der Gleichung

14) $$G(\pi) = \pi^{p^{h-1}(p-1)} \mp \ldots + p = 0 \quad (p)$$

genügt. Da hiernach die Norm von π $(n(\pi) = p)$ von der kleinstmöglichen positiven Ordnung 1 bezüglich p ist, so ist π Primelement bezüglich $\mathfrak{p}$, der Grad von $\mathfrak{p}$ somit gleich 1 und die Ordnung gleich $\varphi(p^h)$. $\mathfrak{p}$ ist Verzweigungsteiler in $\Re_{p^h}$, da sicher $\varphi(p^h) > 1$, und zwar der einzige, da nach Satz 1 die zu Primzahlen $q \neq p$ gehörigen Primteiler keine Verzweigungsteiler sind. ζ ist eine Einseinheit, d. h. $\zeta \equiv 1 \bmod \mathfrak{p}$, was unmittelbar aus $\pi = 1 - \zeta$ folgt.

Wir wollen jetzt noch die Verzweigungsordnung $\bar{e}$ von $\mathfrak{p}$ bestimmen. Darunter versteht man allgemein, wenn $\mathfrak{p}$ ein zu p gehöriger Primteiler f-ten Grades und e-ter Ordnung in einem algebraischen Zahlkörper k ist, die um 1 vermehrte Ordnungszahl von $\psi'(\pi) = \left(\frac{d\psi(x)}{dx}\right)_{x=\pi}$ (bezügl. $\mathfrak{p}$), wobei π ein Primelement bezügl. $\mathfrak{p}$, $\psi(x)$ das im Körper der $(p^f - 1)$-ten Einheitswurzeln über $K(p)$ (dem sog. Koeffizientenkörper von $k(\mathfrak{p})$) irreduzible Polynom e-ten Grades, dem π genügt, bedeutet. (A. Z. S. 219).

In unserem Falle ist der Koeffizientenkörper gleich $K(p)$, da $f = 1$ ist und $K(p)$ die $(p-1)$-ten Einheitswurzeln enthält. (A. Z.

S. 80). Das Primelement $\pi = 1 - \zeta$ ist Wurzel des irreduziblen Polynoms $\varphi(p^h)$-ten Grades

$$G(y) = F_{p^h}(1 - y) = \frac{(1-y)^{p^h} - 1}{(1-y)^{p^{h-1}} - 1} \quad (p).$$

Es ist also:

15) $$[(1-y)^{p^{h-1}} - 1]G(y) = (1-y)^{p^h} - 1 \quad (p).$$

Differenziert man 15) und beachtet, daß $G(\pi) = 0$ (p) und $\zeta = 1 - \pi$, so ergibt sich

16) $$G'(\pi) = -\frac{p^h \zeta^{p^h - 1}}{(1-\pi)^{p^{h-1}} - 1} \sim \pi^{h\varphi(p^h)} - p^{h-1} \sim \pi^{p^{h-1}(hp-h-1)},$$

also

17) $$\bar{e} = p^{h-1}(hp - h - 1) + 1.$$

Somit erhalten wir:

Satz 4. Die Primzahl p gestattet in $\mathfrak{R}_{p^h}$ die Zerlegung $p \sim \mathfrak{p}^{\varphi(p^h)}$. Der Grad von $\mathfrak{p}$ ist 1 und die Ordnung $\varphi(p^h)$. $\mathfrak{p}$ ist der einzige Verzweigungsteiler in $\mathfrak{R}_{p^h}$ und die Verzweigungsordnung ist $\bar{e} = p^{h-1}(hp - h - 1) + 1$. Bezeichnet ζ eine primitive p^h-te Einheitswurzel, so ist $\pi = 1 - \zeta$ ein Primelement bezügl. $\mathfrak{p}$. Die p^h-ten Einheitswurzeln sind Einseinheiten bezügl. $\mathfrak{p}$.[1]).

Weiter ergibt sich aus der allgemeinen Theorie (A. Z. S. 217):

Satz 5. Die $\varphi(p^h)$ Zahlen $1, \pi, \pi^2, \ldots \pi^{\varphi(p^h)-1}$ bilden ein Fundamentalsystem für den Bereich von $\mathfrak{p}$.

Für die Diskriminante D eines algebraischen Zahlkörpers k m-ten Grades hat Herr Hensel den Ausdruck

18) $$D = (-1)^{m-r} n(\mathfrak{Z}) = (-1)^{m-r} \Pi n(\mathfrak{p}^{\bar{e}-1})$$

angegeben. (A. Z. S. 237). Hierbei bedeutet: r die Anzahl der irreduziblen reellen Faktoren, in die das den Körper k definierende Polynom zerfällt, $\mathfrak{Z} = \Pi \mathfrak{p}^{\bar{e}-1}$, wobei das Produkt über alle Verzweigungsteiler von k zu erstrecken ist ($\bar{e}$ Verzweigungsordnung von $\mathfrak{p}$), den sog. Verzweigungsdivisor von k und $n(\mathfrak{Z})$ seine Norm.

---

1) Wir haben das allerdings nur für die primitiven p^h-ten Einheitswurzeln gezeigt, man sieht aber leicht, daß es für sämtliche p^h-ten Einheitswurzeln gilt, da diese ja Potenzen von ζ sind.

In unserem Falle ist $m = \varphi(p^h)$ und $r = \frac{\varphi(p^h)}{2}$, da $F_{p^h}(x)$ nur konjugiert complexe Wurzeln besitzt. Somit ergibt sich für die Diskriminante D_{p^h} von $\mathfrak{K}_{p^h}$:

$$19) \qquad D_{p^h} = (-1)^{\frac{\varphi(p^h)}{2}} p^{p^{h-1}(hp-h-1)}.$$

Man erkennt leicht, daß sgn $D_{p^h} = -1$ für $p^h = 4$ und $p \equiv 3 \bmod 4$, sonst sgn $D_{p^h} = +1$.

Wir erhalten:

Satz 6. Die Diskriminante von $\mathfrak{K}_{p^h}$ ist

$$D_{p^h} = (-1)^{\frac{\varphi(p^h)}{2}} p^{p^{h-1}(hp-h-1)}$$

und zwar sgn $D_{p^h} = -1$ im Falle $p^h = 4$ und $p \equiv 3 \bmod 4$, sonst sgn $D_{p^h} = +1$[1]).

§ 4. Die Zerlegung von p im Falle $n = p^h n'$, $(p, n') = 1$.

Es sei $n = p^h n'$, $(p, n') = 1$ und t' der Exponent, zu dem p mod n' gehört. Da $(p, n') = 1$, so läßt sich jede primitive n-te Einheitswurzel ω als Produkt einer primitiven p^h-ten Einheitswurzel ζ und einer primitiven n'-ten Einheitswurzel ω' darstellen, und umgekehrt stellt jedes derartige Produkt eine primitive n-te Einheitswurzel dar. Der Körper $\mathfrak{K}_n$ kann daher durch Adjunktion von ω' zu $\mathfrak{K}_{p^h}$ erzeugt werden und ist wegen $\varphi(n) = \varphi(p^h)\varphi(n')$ vom Grade $\varphi(n')$ über $\mathfrak{K}_{p^h}$. Daher ist das in $K(1)$ irreduzible Polynom $F_{n'}(x)$ vom $\varphi(n')$-ten Grade, dem ω' genügt, auch irreduzibel in $\mathfrak{K}_{p^h}$. Nach Satz 4 zerfällt p in $\mathfrak{K}_{p^h}$ in $p \sim \mathfrak{p}^{\varphi(p^h)}$, und da $\mathfrak{p}$ vom 1-ten Grade ist, zerfällt nach Satz 3 $\mathfrak{p}$ im Körper $\mathfrak{K}_n = \mathfrak{K}_{p^h}(\omega')$ in $\frac{\varphi(n')}{t'}$ verschiedene Primteiler $\mathfrak{P}_i$ vom Relativgrade t' und der Relativordnung 1, also p in $\frac{\varphi(n')}{t'}$ verschiedene Primteiler vom Grade t' und der Ordnung $\varphi(p^h)$. Jeder dieser Primteiler $\mathfrak{P}_i$ ist, da $\varphi(p^h) > 1$, Verzweigungsteiler in $\mathfrak{K}_n$. Da die Relativordnung von $\mathfrak{P}_i$ bezügl. $\mathfrak{p}$ gleich 1 ist, so ist $\pi = 1 - \zeta$ auch Primelement für jeden Primteiler $\mathfrak{P}_i$. Die irreduzible Gleichung 14) $G(y) = 0$ (p) $\varphi(p^h)$-ten Grades, der π in $K(p)$ genügt, ist auch in dem Koeffizientenkörper von $\mathfrak{K}_n(\mathfrak{P}_i)$ irredu-

1) Vgl. auch D. Hilbert „Die Theorie der algebraischen Zahlkörper". Jahresber. d. deutsch. Math. Ver. Bd 4 § 96 Satz 121.

zibel, da ja, weil $\mathfrak{P}_i$ von $\varphi(p^h)$-ter Ordnung, π auch in ihm einer irreduziblen Gleichung $\varphi(p^h)$-ten Grades genügen muß. Somit ergibt sich wie im vorigen Paragraphen für die Verzweigungsordnung $\bar{e}_i$ jedes Primteilers $\mathfrak{P}_i$:

$$\bar{e}_i = p^{h-1}(hp - h - 1) + 1.$$

Wir erhalten:

Satz 7. Ist $n = p^h n'$, $(p, n') = 1$ und t' der Exponent, zu dem p mod n' gehört, so zerfällt die Primzahl p in $\mathfrak{K}_n$ in $s = \frac{\varphi(n')}{t'}$ verschiedene Primteiler $\mathfrak{P}_i$ vom Grade t' und der Ordnung $\varphi(p^h)$. Die $\mathfrak{P}_i$ sind Verzweigungsteiler in $\mathfrak{K}_n$ und ihre Verzweigungsordnung ist $\bar{e}_i = p^{h-1}(hp - h - 1) + 1$. $\pi = 1 - \zeta$, wobei ζ eine primitive p^h-te Einheitswurzel bedeutet, ist Primelement bezügl. jedes Primteilers $\mathfrak{P}_i$.

Die in der Diskriminante D_n von $\mathfrak{K}_n$ enthaltene Potenz $D(p)$ von p ergibt sich nach 18) offenbar zu

$$20) \qquad D(p) = \prod_{i=1}^{\frac{\varphi(n')}{t'}} n\left(\mathfrak{P}_i^{\bar{e}_i - 1}\right), \qquad ^1)$$

das Produkt erstreckt über alle Primteiler $\mathfrak{P}_i$ von p, also, da $n(\mathfrak{P}_i) = p^{t'}$ ist,

$$21) \qquad D(p) = p^{\varphi(n')\, p^{h-1}(hp - h - 1)}.$$

Sei nun $n = \prod_{l=1}^{v} p_l^{h_l}$ (p_l Primzahl) und $n_l' = \frac{n}{p^{h_l}}$, so ergibt sich nach 18) und 21), da die den Körper $\mathfrak{K}_n$ definierende Gleichung $F_n(x) = 0$ nur konjugiert complexe Wurzeln besitzt, für die Körperdiskriminante:

$$22) \qquad D_n = (-1)^{\frac{\varphi(n)}{2}} \prod_{l=1}^{v} p_l^{\varphi(n_l')p_l^{h_l-1}(h_l p_l - h_l - 1)}.$$

Wir erhalten:

Satz 8. Die Diskriminante von $\mathfrak{K}_n$ ist

$$D_n = (-1)^{\frac{\varphi(n)}{2}} \prod_{l=1}^{v} p_l^{\varphi(n_l')p_l^{h_l-1}(h_l p_l - h_l - 1)},$$

---

1) Das Zeichen n bedeutet hier natürlich die Norm und ist nicht zu verwechseln mit der Zahl n.

wenn $n = \overset{v}{\underset{l=1}{\Pi}} p_l^{h_l}$ und $n_l' = \frac{n}{p_l^{h_l}}$ gesetzt wird[1]).

Weiter beweise ich:

Satz 9. Die $\varphi(p^h)t'$ Zahlen

$$23) \qquad \begin{matrix} 1, \omega', \omega'^2, \ldots \omega'^{t'-1}; & \pi, \pi\omega', & \ldots & \pi\omega'^{t'-1}; \ldots \\ \pi^{\varphi(p^h)-1}, & \pi^{\varphi(p^h)-1}\omega', & \ldots & \pi^{\varphi(p^h)-1}\omega'^{t'-1}, \end{matrix}$$

wobei $\pi = 1 - \zeta$, ζ eine primitive p^h-te und ω' eine primitive n'-te Einheitswurzel bedeutet, bilden ein Fundamentalsystem für den Bereich jedes Primteilers $\mathfrak{P}_i$ von p in $\mathfrak{R}_n$.

Dies erkennt man, wenn man bedenkt, daß in dem von Herrn Hensel A. Z. S. 222 für den Bereich eines beliebigen Primteilers $\mathfrak{p}$ von p f-ten Grades und e-ter Ordnung angegebenen Fundamentalsystem

$$1, \eta, \ldots \eta^{f-1}; \quad \pi, \pi\eta, \ldots \pi\eta^{f-1}; \quad \ldots \pi^{e-1}, \pi^{e-1}\eta, \ldots \pi^{e-1}\eta^{f-1};$$

wo π ein Primelement bezügl. $\mathfrak{p}$ und η eine primitive $(p^f - 1)$-te Einheitswurzel für den Bereich von $\mathfrak{p}$ bedeutet, η durch eine beliebige zum Exponenten f (bezügl. p) passende Einheitswurzel η_0 desselben Bereiches ersetzt werden darf. Denn es wird ja in dem Beweise auf S. 221 unten nur verlangt, daß $1, \eta, \ldots \eta^{f-1}$ ein Fundamentalsystem für den Koeffizientenkörper bilden. Da aber die Diskriminante der irreduziblen Gleichung f-ten-Grades, der die beliebige zum Exponenten f passende Einheitswurzel η_0 in $K(p)$ genügt, p nicht enthält (A. Z. Kap. 8 § 4), so bilden auch $1, \eta_0, \ldots \eta_0^{f-1}$ ein Fundamentalsystem für den Koeffizientenkörper, womit alles bewiesen ist, da in unserem Falle $f = t'$, ω' zum Exponenten t' paßt (bezügl. p) und $\pi = 1 - \zeta$ nach Satz 7 Primelement für den Bereich jedes Primteilers $\mathfrak{P}_i$ von p ist.

Ich will nun noch einen zweiten Beweis für die Zerlegung von p in $\mathfrak{R}_n$ geben, der die Resultate des § 2 nicht voraussetzt.

Es sei

$$24) \qquad F_n(x) = f_1(x)\, f_2(x) \ldots f_s(x) \quad (p)$$

1) Man vergl. hierzu die Abhandlung von Herrn G. Rados: „Die Diskriminante der allgemeinen Kreisteilungsgleichung". Crelles Journal Bd. 131, wo dieses Resultat auf elementarem Wege, ohne zahlentheoretische Voraussetzungen hergeleitet wird. Beim Vergleiche beachte man, daß der dort angegebene Ausdruck erst in den unsrigen übergeführt werden muß.

die Zerlegung der den Körper $\Re_n$ definierenden Funktion $F_n(x)$ in irreduzible Faktoren in $K(p)$ und $f(x)$, dessen Grad μ sei, irgendeiner von ihnen, sodaß also für den $f(x)$ zugeordneten Primteiler $\mathfrak{P}$ vom Grade f und der Ordnung e $ef = \mu$ ist. Ist ferner $\bar{\omega}$ eine Wurzel der Gleichung

$$f(x) = 0 \qquad (p),$$

so sei

$$\bar{\omega} = \bar{\zeta}\,\bar{\omega}' \qquad (\mathfrak{P})$$

die Darstellung von $\bar{\omega}$ durch eine primitive p^h-te und eine primitive n'-te Einheitswurzel für den Bereich von $\mathfrak{P}$. Es bedeute

25) $$1, i_1, \ldots i_{\varphi(p^h)-1}$$

ein vollständiges System ganzer Zahlen, welche kleiner als p^h und relativ prim zu p sind. Dann sind die $\varphi(p^h)t'$ Zahlen

26) $$\bar{\zeta}^i\bar{\omega}', \ \bar{\zeta}^i\bar{\omega}'^p, \ \ldots \ \bar{\zeta}^i\bar{\omega}'^{p^{t'-1}} \qquad (i = 1, i_1, \ldots i_{\varphi(p^h)-1})$$

Wurzeln eines Polynoms $g(x)$ vom Grade $\varphi(p^h)t'$ in $K(p)$, denn ihre elementarsymetrischen Funktionen sind rationale p-adische Zahlen, weil es diejenigen der $\bar{\zeta}^i$ (nach § 3) und diejenigen der $\bar{\omega}', \bar{\omega}'^p, \ldots \bar{\omega}'^{p^{t'-1}}$ (nach Hilfssatz 1) für sich sind. Aus $g(\bar{\omega}) = f(\bar{\omega}) = 0$ (p) und der Irreduktibilität von $f(x)$ folgt $f(x)/g(x)$, also

27) $$\mu = ef \leqq \varphi(p^h)t'.$$

Da in dem Unterkörper $\Re_{p^h}$ von $\Re_n$ $p \sim \mathfrak{p}^{\varphi(p^h)}$ ist, so gilt für die Ordnung e von $\mathfrak{P}$

28) $$e \geqq \varphi(p^h).$$

Da außerdem p in dem Unterkörper $\Re_{n'}$ von $\Re_n$ nach Satz 1 in lauter Primteiler t'-ten Grades zerfällt, muß der Grad f von $\mathfrak{P}$

29) $$f \geqq t'$$

sein, woraus in Verbindung mit 27) und 28) folgt:

30) $$e = \varphi(p^h), \ f = t'.$$

Hieraus ergibt sich ohne weiteres das in Satz 7 ausgesprochene Zerlegungsgesetz. Wir erhalten überdies noch folgenden

Zusatz zu Satz 7. Ist $f(x)$ einer der irreduziblen Faktoren von $F_n(x)$ in $K(p)$ und $\bar{\omega} = \bar{\zeta}\bar{\omega}'$ eine Wurzel der Gleichung $f(x) = 0$ (p), so sind die $\varphi(p^h)t'$ Zahlen

$$\bar{\zeta}^i\bar{\omega}', \ \bar{\zeta}^i\bar{\omega}'^p, \ \ldots \ \bar{\zeta}^i\bar{\omega}'^{p^{t'-1}}$$

ihre sämtlichen Wurzeln, wobei i die Zahlen 25) durchläuft.

Abschnitt II.

Der Zusammenhang der Kummerschen Theorie der idealen Primfaktoren von p in $\mathfrak{R}_n$ mit der p-adischen Primteilertheorie.

Das Ziel der folgenden Untersuchungen ist die Zerlegung von $F_n(x)$ in $K(p)$ mit Hilfe der Kummerschen Theorie der idealen Primfaktoren von p in $\mathfrak{R}_n$ herzuleiten, und umgekehrt diejenigen Sätze, die der Kummerschen Theorie zugrunde liegen, auf p-adischem Wege aus der Zerlegung von $F_n(x)$ in $K(p)$ zu erschließen. Auch hier sind die beiden Fälle $(p, n) = 1$ und p/n zu unterscheiden.

§ 1. Grundzüge der Kummerschen Theorie.

Wir wollen in diesem Paragraphen die Hauptpunkte der Kummerschen Theorie, die man ausführlich in der in der Einleitung (S. 2) erwähnten Abhandlung Kummers (B. Ak.) dargestellt findet, soweit wir sie für unsere Zwecke benötigen, kurz skizzieren. In der Bezeichnungsweise weichen wir dabei aus formalen Gründen zum Teil von der dort gebrauchten ab.

Wir behandeln zuerst den Fall $(p, n) = 1$.

I. $(p, n) = 1$. Bedeutet ω wie seither eine primitive n-te Einheitswurzel, so wird jeder der n-Ausdrücke

$$1) \qquad \tau_k = \omega^k + \omega^{kp} + \omega^{kp^2} + \ldots + \omega^{kp^{t_d - 1}} \qquad (k = 1, 2, \ldots n),$$

wobei t_d der Exponent ist, zu dem p mod $\frac{n}{(n, k)} = \frac{n}{d}$ gehört, nach Kummer eine Periode der Gleichung $x^n = 1$ genannt. Zu jedem Divisor d von n gehört eine Klasse von Perioden, „die zum Divisor d gehörige Klasse", welche alle und nur diejenigen Perioden enthält, für deren Index k $(k, n) = d$ ist. Die Perioden dieser Klasse heißen zum Divisor d gehörige Perioden. Die Anzahl der Perioden der zum Divisor d gehörigen Klasse ist $s_d = \frac{\varphi(\frac{n}{d})}{t_d}$ [1]). Nach dem Vorgange von L. Fuchs [2]) nennen wir

1) Wir setzen im Einklang mit unseren früheren Bezeichnungen $t_1 = t$, $s_1 = s = \frac{\varphi(n)}{t}$.

2) L. Fuchs, „Über die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist". Crelles Journal, Bd. 61.

die zum Divisor 1 gehörige Klasse primitive Klasse, die betreffenden Perioden primitive Perioden der Gleichung $x^n = 1$. Die Perioden der zum Divisor d gehörigen Klasse können danach als primitive Perioden der Gleichung $x^{\frac{n}{d}} = 1$ aufgefaßt werden. Die Perioden einer Klasse sind entweder alle voneinander verschieden oder sämtlich gleich null [1]). Es gelten nun folgende Sätze über die Perioden.

A) Die Perioden der zum Divisor d gehörigen Klasse genügen einer Gleichung

2) $$P_d(x) = 0$$

mit ganzen rationalen Koeffizienten, in welcher der Koeffizient der höchsten Potenz von x gleich 1 ist. (B. Ak. S. 5).

(Es wird sich später ergeben, daß diese Gleichung in $K(1)$ irreduzibel ist mit Ausnahme des Falles, daß sämtliche Perioden der betreffenden Klasse null sind, dann wird nämlich $P_d(x) = x^{s_d}$).

B) Die Kongruenz $P_d(x) = 0 \bmod p$ besitzt stets mindestens eine reale Kongruenzwurzel. (B. Ak. S. 8).

Es sollen

3) $$r_1 = 1,\ r_2,\ \ldots\ r_s \qquad \left(s = \frac{\varphi(n)}{t}\right)$$

sämtliche ganze Zahlen bedeuten, welche kleiner als n, zu n relativ prim und mod n keiner Potenz von p kongruent sind. Dann bilden die s Substitutionen

4) $$\begin{pmatrix}\omega\\ \omega^{r_1}\end{pmatrix},\ \begin{pmatrix}\omega\\ \omega^{r_2}\end{pmatrix},\ \ldots\ \begin{pmatrix}\omega\\ \omega^{r_s}\end{pmatrix},$$

wie man leicht erkennt, eine Gruppe, welche eine Untergruppe der Galoisschen Gruppe von $\mathfrak{R}_n$ (bezügl. $K(1)$) ist, die wir mir G_P bezeichnen. Diese Substitutionen führen τ_1 in sämtliche Perioden $\tau_1,\ \tau_{r_2},\ \ldots\ \tau_{r_s}$ der primitiven Klasse über, und allgemein wird τ_k in $\tau_{r_i k}$ übergeführt, wobei nach Definition der Perioden $r_i k$ auf seinen kleinsten positiven Rest mod n zu reduzieren ist. Auf Grund der Sätze A) und B) definiert Kummer s Funktionen der Perioden

5) $$\psi(\tau_1),\ \psi(\tau_{r_2}),\ \ldots\ \psi(\tau_{r_s}),$$

---

1) B. Ak. S. 5; über die besonderen Bedingungen vgl. man die genannte Fuchssche Abhandlung.

die aus einer unter ihnen durch Anwendung der Substitutionen von G_P hervorgehen. Um Mißverständnisse zu vermeiden, sei besonders betont, daß die $\psi(\tau_{r_i})$ Funktionen sämtlicher Perioden und nicht etwa nur einer einzigen sind, zu welcher Annahme die Schreibweise verleiten könnte. Wir bezeichnen sie nur so, um anzudeuten, daß $\psi(\tau_{r_i})$ $(i = 1, 2, \ldots s)$ aus $\psi(\tau_1)$ ebenso hervorgeht wie τ_{r_i} aus τ_1, nämlich durch die Substitution $\begin{pmatrix} \omega \\ \omega^{r_i} \end{pmatrix}$. Ferner sei noch bemerkt, daß nach dem Kummerschen Bildungsgesetze bei beliebigem, aber festgewähltem ω die mit $\psi(\tau_1)$ zu bezeichnende Funktion und damit auch $\psi(\tau_{r_i})$ eindeutig bestimmt ist (B. Ak. S. 14).

Die für uns und auch im Aufbau der Kummerschen Theorie wichtigste Eigenschaft der Funktionen $\psi(\tau_{r_i})$ ist diejenige, daß mit ihrer Hilfe jeder Periode τ_k für eine beliebige positive ganze Potenz p^m eine ganze rationale Zahl derart zugeordnet werden kann, daß jede rationale Gleichung mit rationalen Koeffizienten in eine richtige Kongruenz mod p^m übergeht, wenn die Perioden durch die ihnen zugeordneten ganzen rationalen Zahlen ersetzt werden. (B. Ak. S. 17)[1]).

Wir bezeichnen die durch $\psi(\tau_1)$ vermittelte Zuordnung mit

6) $$\tau_k \longrightarrow a_k^{(m-1)} \qquad (k = 1, 2, \ldots n),$$

wo die Zahlen $a_k^{(m-1)}$ bis auf Vielfache von p^m eindeutig bestimmt sind, auf die es für das Erfülltsein der zu betrachtenden Kongruenzen nicht ankommt. Wir wollen und können daher $a_k^{(m-1)}$ stets in der Form

7) $$a_k^{(m-1)} = c_k^{(0)} + c_k^{(1)} p + \ldots + c_k^{(m-1)} p^{m-1}$$

annehmen, wo die Koeffizienten $c_k^{(l)}$ Zahlen der Reihe $(0, 1, \ldots p-1)$ sind[2]).

Die durch $\psi(\tau_{r_i})$ vermittelte Zuordnung geht aus 6) ebenso hervor wie τ_{r_i} aus τ_1. Man erhält sie also, wenn man in τ_k ω durch ω^{r_i} ersetzt; sie kann also geschrieben werden:

---

1) Kummer hat dies zwar nur für Gleichungen mit ganzen rationalen Koeffizienten ausgesprochen, aber man sieht leicht, daß dies dann auch für solche mit gebrochenen rationalen Koeffizienten richtig ist.

2) Vgl. auch Kummers Beweis B. Ak. S. 16.

8a) $\tau_{r_i k} \rightarrow a_k^{(m-1)}$

oder, was dasselbe ist, $(k = 1, 2, \ldots n)$

8b) $\tau_k \rightarrow a_{\varrho_i k}^{(m-1)}$,

wo ϱ_i durch $r_i \varrho_i \equiv 1 \bmod n$ bestimmt ist, wie Kummer ausführlich gezeigt hat (B. Ak. S. 11). Die Produkte $r_i k$ bzw. $\varrho_i k$ $(k = 1, 2, \ldots n)$ sind dabei noch auf ihre kleinsten Reste mod n zu reduzieren. Die Zahlen $a_{\varrho_i k}^{(m-1)}$ stellen also diejenige Permutation der $a_k^{(m-1)}$ dar, die man aus 8a) erhält, wenn die $\tau_{r_i k}$ in ihre natürliche Reihenfolge gebracht werden. Wir können daher in leicht verständlicher Weise sagen, die Permutation $a_{\varrho_i k}^{(m-1)}$ entstehe aus $a_k^{(m-1)}$ durch Anwendung der Substitution $\begin{pmatrix} \omega \\ \omega r_i \end{pmatrix}$ von G_P. Wir nennen die Zuordnungen 8a) und 8b), wenn die Zahlen $a_k^{(m-1)}$ in der Form 7) angenommen werden „reduzierte Kummersche Zuordnungen".

Zusammengefaßt gilt also:

C) Jede rationale Gleichung $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ mit rationalen Koeffizienten geht durch die s Zuordnungen $\tau_k \rightarrow a_{\varrho_i k}^{(m-1)}$ $\left(i = 1, 2, \ldots s = \frac{\varphi(n)}{t}\right)$ in die s richtigen Kongruenzen

9) $$F(a_{\varrho_i}^{(m-1)}, a_{\varrho_i 2}^{(m-1)}, \ldots a_{\varrho_i n}^{(m-1)}) \equiv 0 \bmod p^m$$

über. Die Tatsache des Bestehens der s Kongruenzen 9) können wir auch dadurch ausdrücken, daß wir sagen: Die Kongruenz $F(a_1^{(m-1)}, a_2^{(m-1)}, \ldots a_n^{(m-1)}) \equiv 0 \bmod p^m$ ist invariant gegenüber G_P[1]).

Jeder der Funktionen $\psi(\tau_{r_i})$ wird von Kummer ein bestimmter idealer Primfaktor des p in $\mathfrak{R}_n$ in der Art zugeordnet, daß eine ganze Zahl α aus $\mathfrak{R}_n$ durch ihn teilbar heißt, wenn die Kongruenz

10) $$\psi(\tau_{r_i})\alpha \equiv 0 \bmod p$$

erfüllt ist. Allgemeiner heißt α durch ihn m mal teilbar, wenn

11) $$\psi(\tau_{r_i})^m \alpha \equiv 0 \bmod p^m$$ [2])

ist.

---

1) Im Grunde folgt dies natürlich daraus, daß $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ invariant gegenüber G_P ist, da G_P die Galoissche Gruppe des Periodenkörpers, d. i. des Körpers, der durch Adjunktion aller Perioden $\tau_1, \tau_2, \ldots \tau_n$ zu $K(1)$ entsteht, ist. Dies wollen wir jedoch nicht voraussetzen, sondern es wird sich uns später von selbst ergeben.

2) B. Ak. S. 19. Ist außerdem $\psi(\tau_{r_i})^{m+1}\alpha \not\equiv 0 \bmod p^{m+1}$, so heißt α genau m mal durch ihn teilbar.

Diese Bedingung kann nun, wenn α in der Form

12) $$\alpha = \sum_{l=0}^{\varphi(n)-1} x_l \omega^l$$

mit ganzen rationalen Koeffizienten x_l dargestellt wird (was bekanntlich immer eindeutig möglich ist), stets durch t Kongruenzen mod p^m, welche in Bezug auf die Koeffizienten x_l in 12) linear sind, ersetzt werden, wie Kummer ausführlich gezeigt hat. (B. Ak. S. 33).

Es sei jetzt

II. p/n, $n = p^h n'$, $(p, n') = 1$. Als Perioden der Gleichung $x^n = 1$ sind in diesem Falle die Perioden der Gleichung $x^{n'} = 1$ anzusehen. Wegen $(p, n') = 1$ bleibt, wenn nun für n'

$$\omega',\ \tau'_k,\ t',\ s',\ \psi(\tau'_{r_i}) \quad \text{u. s. w.}^{1})$$

die entsprechenden Bedeutungen haben wie

$$\omega,\ \tau_k,\ t,\ s,\ \psi(\tau_{r_i}) \quad \text{u. s. w.}$$

für n im Falle I, für die Perioden und ihre Zuordnungen alles unter I Gesagte sinngemäß gültig.

Bedeutet ζ eine primitive p^h-te Einheitswurzel, so wird von Kummer jeder der Funktionen $\psi(\tau'_{r_i})$ $(i = 1, 2, \ldots s')$ ein idealer Primfaktor des p in $\mathfrak{R}_n$ derart zugeordnet, daß eine ganze Zahl α aus $\mathfrak{R}_n$ durch ihn teilbar heißt, wenn

13) $$\psi(\tau'_{r_i})\alpha \equiv 0 \bmod (1-\zeta)$$

ist. Allgemeiner heißt α durch ihn m mal teilbar, wenn:

14) $$\psi(\tau'_{r_i})^u \alpha \equiv 0 \bmod (1-\zeta)^m,^{2})$$

wo u der Bedingung genügt

$$u\varphi(p^h) > m.$$

Auch hier zeigt Kummer, daß 14) durch eine gewisse Anzahl anderer Kongruenzen ersetzt werden kann. Es gilt nämlich:

Die Bedingung, daß α einen bestimmten Primteiler des p m mal enthält, ist, wenn $m = c\varphi(p^h) + m_0$, $(0 \leq m_0 < \varphi(p^h))$ gesetzt wird, gleichbedeutend mit $m_0 t'$ Kongruenzen mod p^{c+1} und $(\varphi(p^h) - m_0)t'$ Kongruenzen mod p^c, welche in Bezug auf die Koeffizienten x_l von $\alpha = \sum_{l=0}^{\varphi(n)-1} x_l \omega^l$ linear sind. (B. Ak. S. 35).

1) Für $n' = 1$ sind diese Zahlen einfach gleich 1 zu setzen.

2) Ist außerdem $\psi(\tau'_{r_i})^u \alpha \equiv 0 \bmod (1-\zeta)^{m+1}$, so heißt auch hier α genau m mal durch ihn teilbar. B. Ak. S. 25.

Wir werden später sehen, daß diese Bedingungen und ebenso die im Anschluß an 11) genannten nur Spezialfälle eines für beliebige algebraische Zahlkörper geltenden Theorems sind.

§ 2. Uebergang zu den p-adischen Zahlen.

Die Reihe der mit Hilfe von $\psi(\tau_1)$ für $m = 1, 2, \ldots$ gebildeten Zahlen $a_k^{(0)}, a_k^{(1)} \ldots$ definiert unter Berücksichtigung von 7) eine eindeutig bestimmte ganze rationale p-adische Zahl, nämlich

15) $$a_k = \lim_{m=\infty} a_k^{(m-1)} \quad (p),^1)$$

sodaß wir mit Hilfe von $\psi(\tau_1)$ jeder der Perioden τ_k eindeutig eine ganze rationale p-adische Zahl a_k, in Zeichen

16) $$\tau_k \longrightarrow a_k \quad (p) \qquad\qquad (k = 1, 2, \ldots n)$$

derart zuordnen können, daß, wie einfach aus C) unter Berücksichtigung der Definition der Gleichheit in $K(p)$ folgt, der Satz gilt:

Satz 1. Aus der Gleichung $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ folgt vermöge 16) die Gleichung $F(a_1, a_2, \ldots a_n) = 0\ (p)$, und letztere Gleichung ist invariant gegenüber der Gruppe G_P, d. h. mit $F(a_1, a_2, \ldots a_n) = 0\ (p)$ gilt auch $F(a_{\varrho_i}, a_{\varrho_i 2}, \ldots a_{\varrho_i n}) = 0\ (p)$, wobei $a_{\varrho_i k}$ aus a_k durch die Substitution $\begin{pmatrix} \omega \\ \omega' _i \end{pmatrix}$ hervorgeht in demselben Sinne wie früher $a_{\varrho_i k}^{(m-1)}$ aus $a_k^{(m-1)}$ 2).

Ich beweise jetzt die Umkehrung:

Satz 2. Aus $F(a_1, a_2, \ldots a_n) = 0\ (p)$ folgt $F(\tau_1, \tau_2, \ldots \tau_n) = 0$, wenn a_k durch τ_k ersetzt wird, und letztere Gleichung ist invariant gegenüber der Gruppe G_P.

Beweis. Es sei

17) K_P der Periodenkörper (Definition s. Anm. 1 auf S. 17), ϑ ein primitives Element von K_P und

18) $$R(x) = 0$$

die in $K(1)$ irreduzible Gleichung, der ϑ genügt und ferner

19) $$\vartheta = g(\tau_1, \tau_2, \ldots \tau_n),$$

---

1) Der Limesbegriff ist hier im p-adischen Sinne (A. Z. S. 21) zu verstehen.

2) $F(\ldots)$ bedeutet hier und im folgenden stets eine ganze rationale Funktion ihrer Argumente mit gewöhnlichen rationalen Koeffizienten.

wo $g(\tau_1, \tau_2, \ldots \tau_n)$ eine rationale Funktion der Perioden mit rationalen Koeffizienten ist, die Darstellung von ϑ durch $\tau_1, \tau_2, \ldots \tau_n$. Aus

20) $$R(\vartheta) = R(g(\tau_1, \tau_2, \ldots \tau_n)) = 0$$

folgt nach Satz 1 vermöge 16)

21) $$R(g(a_1, a_2, \ldots a_n)) = 0 \quad (p).$$

Da $g(a_1, a_2, \ldots a_n)$ als rationale Funktion der n rationalen p-adischen Zahlen $a_1, a_2, \ldots a_n$ mit rationalen Koeffizienten selbst eine Zahl aus $K(p)$ ist, so hat nach 21) $R(x) = 0$ (p) in $K(p)$ die Wurzel

22) $$\overline{\vartheta} = g(a_1, a_2, \ldots a_n) \quad (p).$$

Ist nun $H(x)$ ein beliebiges Polynom aus $K(1)$ und $H(\vartheta) = 0$, so muß auch $H(\overline{\vartheta}) = 0$ (p) sein und umgekehrt. Denn aus $H(\vartheta) = 0$ folgt, wegen der Irreduktibilität von $R(x)$, $H(x) = R(x)H_1(x)$, also nach 21) und 22) $H(\overline{\vartheta}) = 0$ (p). Ist aber umgekehrt $H(\overline{\vartheta}) = 0$ (p), so hat $H(x)$ mit $R(x)$ in $K(p)$ die Wurzel $\overline{\vartheta}$ gemeinsam. $H(x)$ und $R(x)$ besitzen also einen größten gemeinsamen Teiler für den Bereich von p. Dieser muß, weil nach dem Euklidischen Teilerverfahren bestimmbar, ein Polynom aus $K(1)$ sein, also wegen der Irreduktibilität von $R(x)$ mit $R(x)$ identisch sein, woraus sofort folgt $H(\vartheta) = 0$.

Sei jetzt

23) $$\tau_k = h_k(\vartheta) \qquad (k = 1, 2, \ldots n)$$

die Darstellung von τ_k durch das primitive Element ϑ, wobei $h_k(x)$ ein Polynom aus $K(1)$ ist, so ist

24) $$a_k = h_k(\vartheta) \quad (p) \qquad (k = 1, 2, \ldots n).$$

Denn aus 23) oder $\tau_k - h_k(\vartheta) = 0$ und 19) ergibt sich zunächst $\tau_k - h_k(g(\tau_1, \tau_2, \ldots \tau_n)) = 0$ und hieraus folgt nach Satz 1 $a_k - h_k(g(a_1, a_2, \ldots a_n)) = 0$ (p) also nach 22)

$$a_k = h_k(\vartheta) \quad (p).$$

Sei nun $F(a_1, a_2, \ldots a_n) = 0$ (p), so folgt hieraus zunächst $F(h_1(\vartheta), h_2(\vartheta), \ldots h_n(\vartheta)) = 0$ (p), also nach dem im Anschluß an 22) Bemerkten und 23)

$$F(h_1(\vartheta), h_2(\vartheta), \ldots h_n(\vartheta)) = F(\tau_1, \tau_2, \ldots \tau_n) = 0,$$

womit der erste Teil des Satzes 2 bewiesen ist. Der zweite Teil der Behauptung des Satzes ergibt sich unmittelbar aus der Invarianz von $F(a_1, a_2, \ldots a_n) = 0$ (p) gegenüber G_P.

Auf Grund der Sätze 1 und 2 können wir K_P einen Teilkörper $\overline{K}_P$ von $K(p)$ eineindeutig und isomorph bezügl. $K(1)$ vermöge der Vorschrift:

25) $K(1)$ wird sich selbst zugeordnet
$$\tau_k \longleftrightarrow a_{\varrho_i k} \quad (\tau_{r_i k} \longleftrightarrow a_k)$$

zuordnen, d. h. es läßt sich K_P ein Teilbereich $\overline{K}_P$ von $K(p)$ so zuordnen, daß, wenn α, β und $\bar{\alpha}$, $\bar{\beta}$ zwei Elemente aus K_P bzw. $\overline{K}_P$ bezeichnen, aus $\alpha \longleftrightarrow \bar{\alpha}$, $\beta \longleftrightarrow \bar{\beta}$ folgt:

1. falls $\alpha = \beta$, ist auch $\bar{\alpha} = \bar{\beta}$ und umgekehrt, d. h. daß die Zuordnung eineindeutig ist,

2. $$\alpha + \beta \longleftrightarrow \bar{\alpha} + \bar{\beta}$$
$$\alpha\beta \longleftrightarrow \bar{\alpha}\bar{\beta}.$$

Beweis. Nach Definition ist ja K_P der Bereich aller rationalen Funktionen von $\tau_1, \tau_2, \ldots \tau_n$ mit rationalen Koeffizienten, sodaß sich jedes Element α von K_P in der Form $\alpha = \frac{F(\tau_1, \tau_2, \ldots \tau_n)}{G(\tau_1, \tau_2, \ldots \tau_n)}$ darstellen läßt, wo F und G ganze rationale Funktionen ihrer Argumente mit Koeffizienten aus $K(1)$ sind. Ordnet man nun jedem Element $\alpha = \frac{F(\tau_1, \tau_2, \ldots \tau_n)}{G(\tau_1, \tau_2, \ldots \tau_n)}$ nach 25) ein Element $\bar{\alpha} = \frac{F(a_{\varrho_i}, a_{\varrho_i 2}, \ldots a_{\varrho_i n})}{G(a_{\varrho_i}, a_{\varrho_i 2}, \ldots a_{\varrho_i n})}$ in $K(p)$ zu, so ist der so entstehende Teilbereich $\overline{K}_P$ von $K(p)$ isomorph zu K_P, d. h. die Bedingungen 1 und 2 sind erfüllt, wie unschwer auf Grund der Sätze 1 und 2 (S. 19) zu beweisen ist. Auf die Einzelheiten des Beweises darf wohl verzichtet werden.

Für $i = 1, 2, \ldots s = \frac{\varphi(n)}{t}$ werden durch 25) s Zuordnungen definiert, die K_P offenbar stets denselben Teilkörper $\overline{K}_P$ von $K(p)$ eineindeutig und isomorph, aber in verschiedener Weise, zuordnen.

Die Tatsache, daß K_P zu K_P vermöge 25) isomorph ist, drücken wir durch das Zeichen:

26) $$K_P \underset{(r_i)}{\cong} \overline{K}_P$$

aus, wobei der Index r_i darauf hinweist, durch welche der s Zuordnungen $\tau_k \longleftrightarrow a_{\varrho_i k}$ der Isomorphismus hervorgebracht wurde.

Wir können offenbar auch sagen, der Isomorphismus 26) sei durch die Funktion $\psi(\tau_{r_i})$ erzeugt.

Ich bemerke noch, daß $\overline{K}_P$ ein echter Teilkörper von $K(p)$ ist, denn $\overline{K}_P$ hat ja dieselbe Mächtigkeit wie K_P, ist also abzählbar, während $K(p)$ bekanntlich überabzählbar, nämlich von der Mächtigkeit des Kontinuums ist.

Es sei $\begin{Bmatrix} K_P[x] \\ \overline{K}_P[x] \end{Bmatrix}$ der Integritätsbereich aller ganzen Funktionen von x mit Koeffizienten aus $\begin{Bmatrix} K_P \\ \overline{K}_P \end{Bmatrix}$. Dann ist mit

$$K_P \underset{(r_i)}{\cong} \overline{K}_P$$

auch

27) $$K_P[x] \underset{(r_i)}{\cong} \overline{K}_P[x].$$

Hieraus will ich nun eine einfache Folgerung ziehen. Da $P_d(x)$ nur Koeffizienten aus $K(1)$ enthält [1]), so ist nach 25) $\bar{P}_d(x) = P_d(x)$, wenn $\bar{P}_d(x)$ das $P_d(x)$ in $\overline{K}_P$ zugeordnete Polynom ist. Nun ist aber $P_d(x) = \underset{(k,n)=d}{\Pi} (x - \tau_k)$ in K_P, wegen des Isomorphismus 27) also $P_d(x) = \underset{(k,n)=d}{\Pi} (x - a_{\varrho_i k})$ in $\overline{K}_P$, also auch in $K(p)$. Somit gilt:

Satz 3. Die Gleichung $P_d(x) = 0 \ (p)$ zerfällt in $K(p)$ in Linearfaktoren. Die reduzierten Kummerschen Zuordnungszahlen 7) sind also nichts weiter als die Näherungswerte der p-adischen Entwicklungen der Perioden.

§ 3. Die Zerlegung von $F_n(x)$ in $K(p)$.

I. $(p, n) = 1$.

In diesem Falle genügt jede primitive n-te Einheitswurzel in K_P nebst den anderen mit ihr in einer primitiven Periode enthaltenen Einheitswurzeln einer Gleichung t-ten Grades (B. Ak. S. 31). (Daß diese irreduzibel in K_P ist, wird nachher als Nebenresultat herauskommen). Daher zerfällt die in $K(1)$ irreduzible Funktion $F_n(x)$ in $s = \frac{\varphi(n)}{t}$ Faktoren t-ten Grades in K_P:

28) $$F_n(x) = f(x, \tau_1)\ f(x, \tau_{r_2}) \ \ldots \ f(x, \tau_{r_s}),$$

1) Vgl. S. 15 A).

wobei $f(x, \tau_{r_l})$ diejenige Funktion ist, die alle und nur die in der primitiven Periode τ_{r_l} enthaltenen Einheitswurzeln als Wurzeln enthält. Aus 27) folgt dann sofort, da $F_n(x)$ nur Koeffizienten aus $K(1)$ enthält, eine entsprechende Zerlegung von $F_n(x)$ in $\overline{K}_P$, die wir wie folgt schreiben können:

29) $$F_n(x) = f(x, a_{\varrho_i}) \; f(x, a_{\varrho_i r_2}) \ldots f(x, a_{\varrho_i r_s})^{1}).$$

Dies ist eine Zerlegung von $F_n(x)$ in $s = \frac{\varphi(n)}{t}$ verschiedene p-adische Faktoren t-ten Grades, von denen jetzt noch zu zeigen ist, daß sie in $K(p)$ irreduzibel sind. Die Irreduktibilität dieser Faktoren kann nicht etwa aus derjenigen der Funktionen $f(x, \tau_{r_l})$ in K_P erschlossen werden. Hieraus könnte nur die Irreduktibilität von $f(x, a_{\varrho_i r_l})$ in dem isomorphen $\overline{K}_P$ gefolgert werden, dagegen nicht diejenige in dem umfassenderen Körper $K(p)$. Der Beweis hierfür kann vielmehr nur p-adisch geführt werden. Nun hatten wir aber bereits auf S. 5 gezeigt, daß $F_n(x)$ in $\frac{\varphi(n)}{t}$ verschiedene irreduzible p-adische Faktoren t-ten Grades zerfällt, die wegen der Eindeutigkeit der Zerlegung von $F_n(x)$ in $K(p)$ mit den Faktoren $f(x, a_{\varrho_i r_l})$ in 29) übereinstimmen müssen. Da die Funktionen $f(x, a_{\varrho_i r_l})$ hiernach in $K(p)$ irreduzibel sind, so sind sie es erst recht in dem engeren Bereich K_P, und daher wegen der Isomorphie 27) auch die ihnen zugeordneten Funktionen $f(x, \tau_{r_l})$ in K_P, woraus sich insbesondere ergibt, daß der Kreiskörper vom t-ten Grade über K_P und K_P vom $\frac{\varphi(n)}{t}$-ten Grade über $K(1)$ ist. K_P ist als Unterkörper von $\Re_n$ bekanntlich ein Galoisscher Körper. G_P ist seine Galoissche Gruppe, weil ja die Substitutionen von G_P $s = \frac{\varphi(n)}{t}$ verschiedene Automorphismen von K_P bezügl. $K(1)$ erzeugen, da z. B. $\psi(\tau_1)$ nacheinander in die s verschiedenen Elemente $\psi(\tau_1), \ldots \psi(\tau_{r_s})$ von K_P übergeführt wird.

Wendet man die Isomorphismen 27) für $i = 1, 2, \ldots s$ oder, wie man auch sagen kann, die durch die Funktionen $\psi(\tau_{r_i})(i = 1, 2, \ldots s)$ erzeugten Isomorphismen, nacheinander an, so geht dabei die

---

1) Für $i = 1, 2, \ldots s$ vertauscht sich nur die Reihenfolge der Faktoren von $F_n(x)$.

Funktion $f(x, \tau_1)$, der ω genügt, nacheinander in die s verschiedenen p-adischen Faktoren $f(x, a_1)$, $f(x, a_{\varrho_2})$, $\ldots f(x, a_{\varrho_s})$ über. Bezeichnet $\bar{\omega}_i$ eine Wurzel von $f(x, a_{\varrho_i}) = 0$ (p), so können allgemein sämtliche Wurzeln von $f(x, a_{\varrho_i})$ in der Form

30) $$\bar{\omega}_i, \bar{\omega}_i^p, \ldots \bar{\omega}_i^{p^{t-1}} \qquad \left(i = 1, 2, \ldots s = \frac{\varphi(n)}{t}\right)$$

geschrieben werden. Es werden also der primitiven Wurzel ω durch $\psi(\tau_1), \ldots \psi(\tau_{r_s})$ nacheinander die $\frac{\varphi(n)}{t}$ Wurzelzyklen 30) zugeordnet, d. h., da bei Kummer jeder Funktion $\psi(\tau_{r_i})$ ein Primteiler des p in $\mathfrak{R}_n$ zugeordnet ist, jedem Primteiler des p entspricht ein bestimmter p-adischer Wurzelzyklus, wie es auch nach der p-adischen Theorie sein muß [1]).

II. Sei jetzt p/n, $n = p^h n'$, $(p, n') = 1$.

Der Periodenkörper K_P von $\mathfrak{R}_n$, der in diesem Falle nach unseren früheren Festsetzungen [2]) mit dem Periodenkörper von $\mathfrak{R}_{n'}$ identisch ist, und für den daher wegen $(p, n') = 1$ alles unter I Gesagte gilt, ist vom Grade $s' = \frac{\varphi(n')}{t'}$ über $K(1)$, folglich $\mathfrak{R}_n$ vom Grade $\varphi(p^h)t'$ über K_P (t' der Exponent, zu dem p mod n' gehört). Hieraus folgt, daß ω einer Gleichung $\varphi(p^h)t'$-ten Grades in K_P genügt. $F_n(x)$ zerfällt daher in K_P in $\frac{\varphi(n')}{t'}$ irreduzible Faktoren $\varphi(p^h)t'$-ten Grades. Nun genügen die $\varphi(p^h)t'$ Größen

31) $$\zeta^l \omega'^{r_i}, \ \zeta^l \omega'^{r_i p}, \ \ldots \ \zeta^l \omega'^{r_i p^{t'-1}},$$

wobei ζ eine primitive p^h-te Einheitswurzel bezeichnet, l ein vollständiges System mod p^h inkongruenter zu p teilerfremder ganzer Zahlen durchläuft, $\omega'^{r_i}, \omega'^{r_i p}, \ldots \omega'^{r_i p^{t'-1}}$ die die primitive Periode

32) $$\tau'_{r_i} = \omega'^{r_i} + \omega'^{r_i p} + \ldots \omega'^{r_i p^{t'-1}}$$

zusammensetzenden primitiven n'-ten Einheitswurzeln sind, einer (irreduziblen) Gleichung $\varphi(p^h)t'$-ten Grades in K_P, weil ihre elementarsymmetrischen Funktionen Zahlen aus K_P sind. Wir können daher die Zerlegung von $F_n(x)$ in K_P wie folgt schreiben:

---

1) Vgl. z. B. Cr. J. 136.

2) Vgl. S. 18.

33) $$F_n(x) = f(x, \tau'_1)\, f(x, \tau'_{r_2}) \ldots f(x, \tau'_{r_{s'}}),$$

wo allgemein $f(x, \tau'_{r_i})$ die $\varphi(p^h)t'$ Wurzeln 31) besitzt.

Durch sinngemäße Anwendung unserer früheren Betrachtungen ergibt sich jetzt ohne weiteres, daß durch die $\frac{\varphi(n')}{t'}$ Funktionen $\psi(\tau'_{r_i})$ [1]) $F_n(x)$ in $s' = \frac{\varphi(n')}{t'}$ p-adische Faktoren $\varphi(p^h)t'$-Grades zerlegt werden kann, die nach den Ergebnissen von S. 12 f. in $K(p)$ irreduzibel sind, und daß mit Hilfe von $\psi(\tau'_{r_i})$ $(i = 1, 2, \ldots s')$ der Funktion $f(x, \tau'_1)$, der die primitive n-te Einheitswurzel ω genüge, nacheinander die s' Funktionen, in die $F_n(x)$ in $K(p)$ zerfällt, zugeordnet werden können und damit ω entsprechend jedem Primteiler des p in $\mathfrak{R}_n$ wieder ein bestimmter Wurzelzyklus für den Bereich von p.

III. Ich will jetzt noch den oben in Aussicht gestellten Satz, daß $P_d(x)$, falls die zum Divisor d gehörigen Perioden τ_k $(k, n) = d$ alle verschieden voneinander sind, irreduzibel in $K(1)$ ist, beweisen [2]). Ich brauche dies nur für $d = 1$, also für die Gleichung $s = \frac{\varphi(n)}{t}$-ten Grades, der die primitiven Perioden der Gleichung $x^n = 1$ genügen, zu zeigen. Denn für die anderen folgt es ganz einfach daraus, daß sie als Gleichung der primitiven Perioden der Gleichung $x^{\frac{n}{d}} = 1$ aufgefaßt werden können. Sei also jetzt $d = 1$, so ist ja τ_1 (falls es nicht null) ein zu G_P gehöriges Element von K_P, da es durch G_P in die s verschiedenen Elemente $\tau_1, \tau_{r_2}, \ldots \tau_{r_s}$ übergeführt wird, τ_1 muß also nach der Galoisschen Theorie einer irreduziblen Gleichung s-ten Grades in $K(1)$ genügen, $P_1(x)$ also irreduzibel sein.

§ 4. Eindeutigkeit der Kummerschen Zuordnungen.

Wir hatten gesehen, daß man jeder Periode τ_k eine ganze rationale p-adische Zahl a_k so zuordnen kann, daß 1: jede Gleichung $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ mit rationalen Koeffizienten auch für den Bereich von p gültig ist, falls man die Perioden τ_k durch a_k ersetzt und umgekehrt, und daß 2: $F(a_1, a_2, \ldots a_n) = 0$ (p) (bezw. $F(\tau_1, \tau_2, \ldots \tau_n) = 0$) invariant gegenüber G_P ist. Ich will jetzt

1) Definition von $\psi(\tau'_{r_i})$ s. S. 18.

2) Vgl. S. 15 A).

zeigen, daß diese beiden Eigenschaften charakteristisch für diese Zuordnungen sind, d. h. wenn uns irgendeine Zuordnung $\tau_k \longleftrightarrow b_k$ der Perioden und rationalen p-adischen Zahlen mit diesen beiden Eigenschaften gegeben ist, so ist die Gesamtheit aller Zuordnungen, die man aus $\tau_k \longleftrightarrow b_k$ durch Anwendung von G_P erhält, mit der Gesamtheit der Zuordnungen, die man aus $\tau_k \longleftrightarrow a_k$ durch Anwendung von G_P erhält, identisch. Dazu habe ich zu zeigen,

1. daß die Zahlen b_k $(k = 1, 2, \ldots n)$ abgesehen von der Reihenfolge mit den Zahlen a_k $(k = 1, 2, \ldots n)$ übereinstimmen,

2. daß die Zahlen a_k nur in den besprochenen s Permutationen den Perioden τ_k zugeordnet werden können.

ad 1. Ist $\tau_k \longleftrightarrow b_k$ eine solche Zuordnung, so zeigt man genau, wie für die a_k (S. 22) daß

$$P(x) = \prod_{d|n} P_d(x) = \prod_{k=1}^{n} (x - b_k) \quad (p)$$

ist. Hieraus folgt ohne weiteres, daß die b_k, abgesehen von der Reihenfolge, mit den a_k übereinstimmen müssen.

ad. 2. Sei $\tau_{r'k} \longleftrightarrow a_k$, wobei $\tau_{r'k}$ eine von den s Permutationen $\tau_{r_i k}$ $(i = 1, 2, \ldots s)$ verschiedene Anordnung der τ_k ist, so folgte nach unseren Voraussetzungen aus $F(a_1, a_2, \ldots a_n) = 0$ (p), daß $F(\tau_{r'}, \tau_{r'2}, \ldots \tau_{r'n}) = 0$. Dies bedeutete, daß die Gleichung $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ nicht nur bei G_P invariant ist, was unmöglich ist, da G_P die Galoissche Gruppe des Periodenkörpers K_P ist. Wir können also sagen:

Satz 4. Es gibt nur ein einziges System ganzer rationaler p-adischer Zahlen $a_1, a_2, \ldots a_n$, die den n Perioden $\tau_1, \tau_2, \ldots \tau_n$ so zugeordnet werden können, daß aus $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ folgt $F(a_1, a_2, \ldots a_n) = 0$ (p) und umgekehrt, und letztere Gleichung invariant gegenüber den Substitutionen der Gruppe G_P ist. Es gibt nur $s = \frac{\varphi(n)}{t}$ verschiedene Zuordnungen zwischen diesen Zahlen und den Perioden mit diesen Eigenschaften, und alle gehen aus einer von ihnen durch Anwendung von G_P hervor.

Die Zahlen und die Zuordnungen sind also durch diese beiden Eigenschaften eindeutig bestimmt. Aus der Definition der Gleichheit in $K(p)$ folgt weiter, daß auch die reduzierten Kummerschen

Zuordnungen durch die in C) (S. 17) ausgesprochenen Eigenschaften eindeutig bestimmt sind.

Kummer hat gezeigt, daß es nach seinem für die Funktionen 5) $\psi(\tau_{r_i})$ angegebenen Bildungsgesetz keine anderen Funktionen der Perioden mit den im Bildungsgesetz für die $\psi(\tau_{r_i})$ verlangten Eigenschaften mehr gibt. (B. AK. S. 14). Danach wäre es aber a priori trotzdem möglich, daß es noch Zuordnungen von Perioden und rationalen Zahlen gibt, welche die in C) verlangten Eigenschaften haben, oder daß es Funktionen der Perioden gäbe, die nach einem anderen als dem Kummerschen Bildungsgesetz erzeugt, andere Zuordnungen mit den verlangten Eigenschaften stifteten. Dies ist aber nach dem soeben Bewiesenen nicht möglich und hiermit die Kummersche Theorie in einem Punkte ergänzt.

§ 5. Herleitung der Kummerschen Zuordnungen aus der Zerlegung von $F_n(x)$ in $K(p)$.

Wir wollen jetzt die Kummerschen Zuordnungen aus der im Abschnitt I gefundenen Zerlegung von $F_n(x)$ in $K(p)$

$$F_n(x) = f_1(x)\ f_2(x)\ \ldots\ f_s(x) \quad (p)$$

auf p-adischem Wege herleiten. Wir gehen davon aus, daß jeder beliebigen, aber fest gewählten primitiven n-ten Einheitswurzel ω, ebenso wie jeder anderen Zahl aus $\mathfrak{R}_n$ eindeutig $\varphi(n)$ Zahlen in jedem der unendlich vielen äquivalenten Wurzelkörper von $F_n(x)$ über $K(p)$ zugeordnet werden können[1]), welche in ebensoviele Zyklen p-adischer algebraischer Zahlen zerfallen, wie $F_n(x)$ irreduzible Faktoren in $K(p)$ besitzt. Wir legen der Betrachtung einen beliebigen, aber fest gewählten dieser Wurzelkörper zugrunde, den wir mit W bezeichnen. Die $\varphi(n)$ zu ω gehörigen Zahlen in W sind die Wurzeln von $F_n(x)$ in W.

I. Sei zuerst $(p, n) = 1$. Dann können die Wurzeln der Funktion $F_n(x)$ in W, wenn

$$\varrho_1 = 1,\ \varrho_2,\ \ldots\ \varrho_s \qquad \left(s = \frac{\varphi(n)}{t}\right)$$

1) Unter Wurzelkörper von $F_n(x)$ über $K(p)$ verstehen wir im Sinne von Cr. J. 136 jede Erweiterung niedrigsten Grades von $K(p)$, in der $F_n(x)$ in Linearfaktoren zerfällt. Allgemein heißen zwei algebraische Erweiterungen $K(p, \delta)$ und $K(p, \bar{\delta})$ äquivalent, wenn in ihnen zwei primitive Elemente β und β existieren, welche beide Wurzeln derselben in $K(p)$ irreduziblen Gleichung sind (Cr. J. 136 S. 190).

ein vollständiges System mod n inkongruenter zu n teilerfremder ganzer Zahlen, welche keiner Potenz von p mod n kongruent sind, und $\bar{\omega}$ eine Wurzel von $f_1(x) = 0\ (p)$ bedeutet, wie folgt angeordnet werden

34) $\bar{\omega}, \bar{\omega}^p, \ldots \bar{\omega}^{p^{t-1}}; \bar{\omega}^{\varrho_2}, \bar{\omega}^{\varrho_2 p}, \ldots \bar{\omega}^{\varrho_2 p^{t-1}}; \ldots \bar{\omega}^{\varrho_s}, \bar{\omega}^{\varrho_s p}, \ldots \bar{\omega}^{\varrho_s p^{t-1}};$

sodaß allgemein

35) $$\bar{\omega}^{\varrho_i}, \bar{\omega}^{\varrho_i p}, \ldots \bar{\omega}^{\varrho_i p^{t-1}} \quad \left(i = 1, 2, \ldots s = \frac{\varphi(n)}{t}\right)$$

einen Zyklus konjugierter Wurzeln bildet. Es werde mit $f_i(x)$ derjenige Faktor von $F_n(x)$ bezeichnet, der die Wurzeln 35) besitzt.

Jedem der $s = \frac{\varphi(n)}{t}$ Wurzelzyklen 35) entspricht nach Hensels Theorie ein Primteiler $\mathfrak{p}_i$ des p in $\mathfrak{R}_n$. Wir können nun ohne Beschränkung der Allgemeinheit

36) $$\omega = \bar{\omega}^{\varrho_i} \ (\mathfrak{p}_i) \qquad (i = 1, 2, \ldots s)$$

für den Bereich von $\mathfrak{p}_i$ setzen, wo also $\bar{\omega}^{\varrho_i}$ eine Zahl des zu $\mathfrak{p}_i$ gehörigen Wurzelzyklus von ω ist[1]). Dann gilt für die n Perioden τ_k

37) $$\tau_k = \omega^k + \omega^{kp} + \ldots \omega^{kp^{t_d-1}} = \bar{\omega}^{\varrho_i k} + \bar{\omega}^{\varrho_i kp} + \ldots \bar{\omega}^{\varrho_i kp^{t_d-1}} = b_{\varrho_i k} \ (\mathfrak{p}_i), \quad (i = 1, 2, \ldots s)$$

wobei $b_{\varrho_i k}$ als elementar-symmetrische Funktion eines Zyklus konjugierter zum Exponenten t_d (bezügl. p) passender Einheitswurzeln eine ganze rationale p-adische Zahl ist. (Hätte man $\omega = \bar{\omega}^{\varrho_i p^l}\ (\mathfrak{p}_i)$ gesetzt, wo $\bar{\omega}^{\varrho_i p^l}$ eine andere Zahl desselben Wurzelzyklus ist, so würde offenbar an dem Werte von $b_{\varrho_i k}$ nichts geändert).

Insbesondere hat man also

38) $$\tau_k = b_k \quad (\mathfrak{p}_1)$$

Da $\bar{\omega}$ eine primitive n-te Einheitswurzel ist, so kann offenbar in $b_{\varrho_i k}$ $\varrho_i k$ auf seinen kleinsten positiven Rest mod n reduziert werden, sodaß also $b_{\varrho_i k}$ eine Permutation der Zahlen b_k darstellt. Schreibt man in 37) die $b_{\varrho_i k}$ in ihrer natürlichen Reihenfolge, dann geht τ_k in $\tau_{r_i k}$ über, wo r_i bestimmt ist durch $r_i \varrho_i \equiv 1 \bmod n$, so-

1) Allgemeiner kann man $\omega = \bar{\omega}^{\varrho_i p^l}\ (\mathfrak{p}_i)$ setzen, wo $\bar{\omega}^{\varrho_i p^l}$ irgendeine der t Zahlen des zu $\mathfrak{p}_i$ gehörigen Wurzelzyklus von ω ist. Man vergl. hierzu besonders A. Z. Kap. XII.

daß also mit 37) gleichbedeutend ist: $\tau_{r_i k} = b_k \ (\mathfrak{p}_i)$. Man erhält also jede der s Relationen 37), indem man nach unserer früheren Ausdrucksweise auf eine von ihnen die Gruppe G_P anwendet. Nach der allgemeinen p-adischen Theorie bleibt nun jede rationale Gleichung mit gewöhnlichen rationalen Koeffizienten zwischen den Perioden

39) $$F(\tau_1, \tau_2, \ldots \tau_n) = 0$$

auch für den Bereich von $\mathfrak{p}_i$ richtig, wenn man τ_k durch $b_{\varrho_i k}$ ersetzt und umgekehrt. Da die $b_{\varrho_i k}$ rationale p-adische Zahlen sind, so können wir dies auch so ausdrücken:

Satz 5. Die Gleichung $F(\tau_1, \tau_2, \ldots \tau_n) = 0$ bleibt richtig in $K(p)$, wenn man τ_k durch $b_{\varrho_i k}$ ersetzt und umgekehrt. Beide Gleichungen sind invariant gegenüber G_P.

Nach Satz 4 (S. 26) müssen daher die den $\mathfrak{p}_i$ entsprechenden Zuordnungen $\tau_k \longleftrightarrow b_{\varrho_i k}$ mit den früheren, durch $\psi(\tau_{r_i})$ erzeugten Zuordnungen $\tau_k \longleftrightarrow a_{\varrho_i k}$ identisch sein.

Aus Satz 5 ergibt sich unter Berücksichtigung des Gleichheitsbegriffes in $K(p)$ der Satz C) des § 1, auf dem Kummers Theorie im wesentlichen beruht.

II. Im Falle $n = p^h n'$, $(p, n') = 1$ ergibt sich die Existenz der $s' = \frac{\varphi(n')}{t'}$ Kummerschen Zuordnungen einfach aus der Tatsache, daß die Perioden von $\mathfrak{R}_n$ gleich denen von $\mathfrak{R}_{n'}$ sind, für sie also das unter I Gesagte sinngemäß anwendbar ist. Das einzige, was uns noch zu zeigen bleibt, ist, daß diese s' Zuordnungen wirklich den Primteilern des p in $\mathfrak{R}_n$ und nicht nur denen des p in $\mathfrak{R}_{n'}$ entsprechen. Dies folgt aber unmittelbar daraus, daß die primitive n'-te Einheitswurzel ω' in $\mathfrak{R}_n$ der Hauptgleichung $(F'_{n'}(x))^{\varphi(p^h)} = 0$ genügt, welche in $K(p)$ in folgender Weise zerfällt:

40) $$(F_{n'}(x))^{\varphi(p^h)} = (f'_1(x))^{\varphi(p^h)} (f'_2(x))^{\varphi(p^h)} \ldots (f'_{s'}(x))^{\varphi(p^h)} \quad (p),$$

wenn

$$F_{n'}(x) = f'_1(x) f'_2(x) \ldots f'_{s'}(x) \quad (p)$$

die Zerlegung von $F_{n'}(x)$ in irreduzible Faktoren in $K(p)$ ist, und nach der allgemeinen Theorie jedem Primteiler des p in $\mathfrak{R}_n$ ein bestimmter der Faktoren $(f'_i(x))^{\varphi(p^h)}$ von 40), also, da es für die Perioden nur auf die irreduziblen Faktoren ankommt, ein bestimmter Faktor $f'_i(x)$ entspricht.

§ 6. Verallgemeinerung der „Kummerschen Kongruenzbedingungen für die Teilbarkeit einer ganzen Zahl aus $\mathfrak{R}_n$ durch eine Primteilerpotenz“ auf den Fall eines beliebigen algebraischen Zahlkörpers.

Es sei k ein beliebiger algebraischer Zahlkörper, λ sein Grad und

41) $$\gamma_1, \gamma_2, \cdots \gamma_\lambda$$

ein absolutes Fundamentalsystem für die ganzen Zahlen in k, sodaß also jede ganze Zahl α aus k in der Form

42) $$\alpha = \sum_{l=1}^{\lambda} x_l \gamma_l$$

mit ganzen rationalen Koeffizienten x_l eindeutig dargestellt werden kann. Ich will jetzt folgenden Satz beweisen:

Satz 6. Sei $\mathfrak{p}$ ein beliebiger Primteiler f-ten Grades und e-ter Ordnung der rationalen Primzahl p in k, m eine beliebige positive ganze rationale Zahl und werde $m = ce + m_0$ $(0 \leqq m_0 < e)$ gesetzt. Dann ist für die Teilbarkeit einer ganzen Zahl α aus k durch $\mathfrak{p}^m$ stets das Erfülltsein von $m_0 f$ Kongruenzen mod p^{c+1} und $(e - m_0)f$ Kongruenzen mod p^c, welche in Bezug auf die x_l in 42) linear sind, notwendig und hinreichend.

Beweis. Sei π ein Primelement bezügl. $\mathfrak{p}$, η_i eine primitive $(\mathfrak{p}^f - 1)$-te Einheitswurzel in $k(\mathfrak{p})$, so bilden die ef Zahlen

43) $$1, \eta, \eta^2, \ldots \eta^{f-1};\ \pi, \pi\eta, \ldots \pi\eta^{f-1};\ \ldots \pi^{e-1}, \pi^{e-1}\eta, \ldots \pi^{e-1}\eta^{f-1}$$

ein Fundamentalsystem für den Bereich von $\mathfrak{p}$. Jede der λ ganzen Zahlen 41) läßt sich nun für den Bereich von $\mathfrak{p}$ durch 43) eindeutig in der Form

44) $$\gamma_i = b_{i,0} + b_{i,1}\eta + \ldots b_{i,f-1}\eta^{f-1} + b_{i,f}\pi + \ldots + b_{i,ef-1}\pi^{e-1}\eta^{f-1} \ (\mathfrak{p}) \quad (i = 1, 2, \ldots \lambda)$$

mit ganzen rationalen p-adischen Koeffizienten $b_{i,k}$ darstellen. Denkt man dies getan, so erhält man aus 42) für α die Darstellung

45) $$\alpha = c_0 + c_1\eta + \ldots c_{f-1}\eta^{f-1} + c_f\pi + \ldots + c_{2f-1}\pi\eta^{f-1} + \ldots + c_{ef-1}\pi^{e-1}\eta^{f-1} \ (\mathfrak{p}),$$

wo die Koeffizienten c_k ihrer Herstellung gemäß ganze rationale p-adische Zahlen sind, welche als Funktionen der x_l in 42) betrachtet, linear sind. Setzt man nun $m = ce + m_0$ $(0 \leqq m_0 < e)$, so

folgen, wie eine einfache Rechnung zeigt, in der Tat aus 45) für die Teilbarkeit von α durch $\mathfrak{p}^m$ die im Satze ausgesprochenen Kongruenzbedingungen.

Satz 6 stellt die auf S. 19 in Aussicht gestellte Verallgemeinerung der von Kummer für den Fall des Kreiskörpers $\mathfrak{K}_n$ angegebenen Kongruenzbedingungen dar, wie man erkennt, wenn man für e und f die speziellen Werte für Primteiler des Kreiskörpers $\mathfrak{K}_n$ einsetzt.

Schließlich sei noch bemerkt, daß aus Satz 6 die Endlichkeit der Anzahl der Idealklassen von k in ähnlicher Weise gefolgert werden kann, wie Kummer dies speziell für den Fall des Kreiskörpers getan hat[1]).

1) B. Ak. §§ 9 u. 10.

II. Teil.

Zerlegung von Primteilern eines algebraischen Zahlkörpers in einem durch ein beliebiges irreduzibles Binom definierten Oberkörper.

---

§ 1. Einleitende Hilfsbetrachtungen.

Es sei k ein beliebiger Körper algebraischer Zahlen, $\mathfrak{p}$ ein Primteiler f-ten Grades und e-ter Ordnung in k, welcher zur rationalen Primzahl p gehöre und $x^n - A$ ein beliebiges irreduzibles Binom aus k. Wir wollen die Zerlegung von $\mathfrak{p}$ in dem durch eine Wurzel x der Gleichung

1) $$x^n = A$$

definierten Oberkörper $k(x)$ über k kennen lernen. Dazu haben wir die Zerlegung von $x^n - A$ in dem Körper $k(\mathfrak{p})$ zu betrachten.

Bedeutet π ein Primelement bezügl. $\mathfrak{p}$, d. h. eine nur durch die erste Potenz von $\mathfrak{p}$ teilbare Zahl aus k, w eine primitive $(p^f - 1)$-te Einheitswurzel in $k(\mathfrak{p})$, so läßt sich die Grundzahl A für den Bereich von $\mathfrak{p}$ eindeutig in der Form

$$A = \pi^a w^b \varepsilon \quad (\mathfrak{p})$$

darstellen, wo a, die Ordnungszahl, und b, der Index von A bezügl. $\mathfrak{p}$, ganze rationale Zahlen sind $(0 \leq b < p^f - 1)$ und ε eine sog. Einseinheit in $k(\mathfrak{p})$, d. h. $\varepsilon \equiv 1 \bmod \mathfrak{p}$ ist. Bei der Behandlung unseres Problems darf nun das primitive Element x der Grundgleichung

2) $$x^n = A = \pi^a w^b \varepsilon \quad (\mathfrak{p})$$

durch ein beliebiges anderes primitives Element x' desselben Körpers ersetzt werden, z. B. durch

$$x' = \alpha + \beta x, \; x' = \tau x, \; x' = x^r,$$

wo α, β, τ beliebige Zahlen aus $k(\mathfrak{p})$ sind, und $(r, n) = 1$ ist, wie Herr Hensel (Cr. J. 151 S. 113) ausführlich gezeigt hat. Setzt man etwa $x' = \pi^{a'} w^{b'} x$, so geht 2) über in

$$x'^n = \pi^{a + a'n} w^{b + b'n} \varepsilon \quad (\mathfrak{p}),$$

und man erkennt, daß durch geeignete Wahl von a' und b' a und b auf ihre kleinsten positiven Reste a_0 bezw. b_0 mod n reduziert werden können, sodaß die zu untersuchende Gleichung in der Form

2a) $$x^n = \pi^{a_0} w^{b_0} \varepsilon \quad (\mathfrak{p})$$

angenommen werden kann.

Ist nun $(p, n) = 1$, so kann diese Gleichung noch weiter vereinfacht werden, da dann, wie ich gleich zeigen werde, zu jeder Einseinheit ε aus $k(\mathfrak{p})$ eine andere Einseinheit ε_0 in $k(\mathfrak{p})$ existiert, für die $\varepsilon_0^n = \varepsilon$ $(\mathfrak{p})$, ε also stets n-ter Potenzrest bezügl. $\mathfrak{p}$ ist und daher durch die Substitution $x' = \frac{x}{\varepsilon_0}$ 2a) in die gleichbedeutende Gleichung

2b) $$x'^n = \pi^{a_0} w^{b_0} \quad (\mathfrak{p})$$

übergeführt werden kann. Es gilt nämlich:

a) $x^n - \varepsilon \equiv x^n - 1 \mod \mathfrak{p}$

b) $x^n - 1 \equiv (x - 1) F(x) \mod \mathfrak{p}$.

Da die Diskriminante $D(x^n - 1)$ im Falle $(p, n) = 1$ $\mathfrak{p}$ nicht enthält, so gilt dasselbe für die Resultante $R((x - 1), F(x))$. Die Funktionen $x - 1$ und $F(x)$ sind daher teilerfremd mod $\mathfrak{p}$. Nun hat Herr Hensel ganz allgemein gezeigt, daß, falls eine ganze ganzzahlige $\mathfrak{p}$-adische Funktion mod $\mathfrak{p}$ in mod $\mathfrak{p}$ teilerfremde Faktoren niedrigeren Grades zerfällt, sie auch für den Bereich von $\mathfrak{p}$ in ebensoviele teilerfremde Faktoren derselben Grade, deren Näherungswerte mod $\mathfrak{p}$ die vorigen Faktoren sind, zerfällt[1]). Der Zerlegung b) entspricht daher die Zerlegung $x^n - \varepsilon = (x - \varepsilon_0) \overline{F}(x)$ $(\mathfrak{p})$, wo $\varepsilon_0^n = \varepsilon$ $(\mathfrak{p})$, $\varepsilon_0 \equiv 1 \mod \mathfrak{p}$ und $F(x) \equiv \overline{F}(x) \mod \mathfrak{p}$ ist. q. e. d.

Ist dagegen p/n, so ist auch $p/D(x^n - 1)$, und es versagt in diesem Falle die obige Beweisführung. In der Tat ist auch dann

1) M. Z. 2 S. 441, 449.

im allgemeinen ε nicht n-ter Potenzrest bezügl. $\mathfrak{p}$, wie hier nicht weiter gezeigt werden soll[1]). In letzterem Falle kann die zu untersuchende Gleichung daher auch nicht in der einfachen Form 2b) geschrieben werden. Ich will mich daher in dieser Abhandlung auf den Fall $(p, n) = 1$ beschränken.

Sei also jetzt stets $(p, n) = 1$. Die Gleichung 2b) läßt sich nun für unsere Zwecke noch etwas weiter vereinfachen. Dazu führe ich folgendes Zeichen ein:

Es bedeute (h, g^{∞}), wo h und g beliebige ganze rationale Zahlen sind, den größten Teiler von h, welcher nur aus in g enthaltenen Primzahlen besteht.

Wir setzen

3) $N = (p^f - 1, n^{\infty})$, $p^f - 1 = NP$, also $(P, N) = 1$, $(P, n) = 1$.

Da der Körper $k(\mathfrak{p})$ die $(p^f - 1)$-ten Einheitswurzeln enthält, so enthält er auch die N-ten und P-ten Einheitswurzeln. Wegen $(P, N) = 1$ läßt sich die primitive $(p^f - 1)$-te Einheitswurzel w in der Form $w = \eta_1 \bar{\eta}_1$ $(\mathfrak{p})$ darstellen, wo η_1 eine primitive N-te und $\bar{\eta}_1$ eine primitive P-te Einheitswurzel in $k(\mathfrak{p})$ bedeutet. 2b) kann daher geschrieben werden

$$x'^n = \pi^{a_0} \eta_1^{b_0} \bar{\eta}_1^{b_0} \quad (\mathfrak{p}).$$

Setzt man $\bar{x} = x' \bar{\eta}_1^{b'}$, so wird $\bar{x}^n = \pi^{a_0} \eta_1^{b_0} \bar{\eta}_1^{b_0 + b'n}$ $(\mathfrak{p})$. Da $(P, n) = 1$, so kann durch geeignete Wahl von b' $b_0 + b'n = 0 \bmod P$ gemacht werden, und die zu untersuchende Gleichung also stets in der Form

4) $$x^n = \pi^{a_0} \eta_1^{b_0} \quad (\mathfrak{p})$$

angenommen werden (wenn wir wieder x statt $\bar{x}$ schreiben). Ist speziell $N = 1$, so ist η_1 einfach gleich 1 zu setzen, und die zu untersuchende Gleichung hat dann die noch einfachere Form

$$x^n = \pi^{a_0} \quad (\mathfrak{p}).$$

Der Exponent b_0 in 4) kann und soll hierbei kleiner als die kleinere der beiden Zahlen n und N angenommen werden. Diesen Exponenten b_0 nennen wir den reduzierten Index von A bezügl. $\mathfrak{p}$ (er ist also nicht immer der kleinste Rest von b mod n, sondern der Rest dieses Restes nach N) und a_0 die reduzierte Ordnungs-

1) Man kann dies sehr einfach zeigen, wenn man die von Herrn Hensel in Cr. J. 146 gegebene Exponentialdarstellung der Einseinheiten benutzt.

zahl von A bezügl. $\mathfrak{p}$. Die Darstellung 4) nennen wir die reduzierte Darstellung der Grundgleichung 2).

Für die weitere Untersuchung haben wir folgende drei Fälle zu unterscheiden:

I. $(a_0, n) = 1$, II. $(a_0, n) = n$ d. h. $a_0 = 0$, III. $(a_0, n) = n' \gtrless \frac{1}{n}$.

Dann ist auch beziehentlich $(a, n) = 1$, $(a, n) = n$, $(a, n) = n'$.

Bevor ich mit der Untersuchung dieser Fälle beginne, will ich noch folgenden Hilfssatz beweisen.

Hilfssatz. Sei g irgendeine ganze rationale Zahl, δ eine primitive g-te Einheitswurzel und h eine nur aus in g enthaltenen Primzahlen bestehende ganze rationale Zahl, so sind sämtliche Wurzeln der Gleichung $x^h = \delta$ primitive hg-te Einheitswurzeln.

Beweis. Sei x irgendeine Wurzel der Gleichung $x^h = \delta$, und r der kleinste Exponent, für den $x^r = 1$, dann folgt aus $x^{hg} = \delta^g = 1$, daß $r | hg$ sein muß. Nun muß aber, wie aus $1 = x^r = (x^r)^h = (x^h)^r = \delta^r$ folgt, r ein Vielfaches von g sein (weil δ primitive g-te Einheitswurzel sein sollte). Also $r = r_0 g$, $r_0 | h$. Sei nun $h = h_0 r_0$. Aus $x^r = x^{r_0 g} = 1$ und der Bedeutung von r folgt dann, daß x^{r_0} eine primitive g-te Einheitswurzel sein muß. Nach Voraussetzung soll aber $\delta = x^h = (x^{r_0})^{h_0}$ ebenfalls eine primitive g-te Einheitswurzel sein, was da h_0 nur aus in g enthaltenen Primzahlen besteht, nur möglich ist, wenn $h_0 = 1$ also $r_0 = h$, $r = hg$ ist. q. e. d.

§ 2. Die Zerlegung von $\mathfrak{p}$ in $k(x)$. (Im Falle $(p, n) = 1$).

I. $(a, n) = (a_0, n) = 1$.

In diesem Falle kann die reduzierte Grundgleichung 4) in der Form

5) $$x'^n = \pi \eta^c \quad (\mathfrak{p})$$

geschrieben werden. Bestimmt man nämlich die ganzen Zahlen r und r' so, daß $r'n + ra_0 = 1$, was wegen $(a_0, n) = 1$ stets möglich ist, so geht durch die Substitution $x' = \pi^r x^r$ 4) über in $x'^n = \pi^{r'n + ra_0} \eta^{b_0 r} = \pi \eta^c$, womit die Behauptung bewiesen ist. Die Gleichung 5) ist eine Eisensteinsche Gleichung, deren konstantes Glied nur durch die erste Potenz von $\mathfrak{p}$ teilbar ist. Sie ist also in $k(\mathfrak{p})$ irreduzibel, und $\mathfrak{p}$ besitzt daher nur einen einzigen Primteiler

$\mathfrak{P}$ in $k(x)$. x' ist selbst Primelement bezügl. $\mathfrak{P}$, weil ja die Norm $n(x')$ nach 5) die kleinstmögliche positive Ordnungszahl 1 bezügl. $\mathfrak{p}$ hat. Der Relativgrad von $\mathfrak{P}$ ist also gleich 1 und die Relativordnung gleich n. Somit gilt:

Satz 1. Ist die Ordnungszahl a von A bezügl. $\mathfrak{p}$ zu n teilerfremd, so besitzt $\mathfrak{p}$ in $k(x)$ die Zerlegung $\mathfrak{p} \sim \mathfrak{P}^n$, wo $\mathfrak{P}$ vom Relativgrade 1 und der Relativordnung n ist [1]).

II. $$(a, n) = (a_0, n) = n, \text{ d. h. } a_0 = 0.$$

Die reduzierte Gleichung 4) lautet in diesem Fall

6) $$x^n = \eta^{b_0} \quad (\mathfrak{p}).$$

Wir setzen

7) $$(b_0, N) = \bar{b}, \; N = \bar{b}N_1, \; b_0 = \bar{b}b_1; \; (b_1, N_1) = 1,$$

dann ist $\eta^{b_0} = \eta^{\bar{b}b_1}$ eine primitive N_1-te Einheitswurzel; ferner sei

8) $$(n, N_1^\infty) = Q, \; n = Qn_1; \; (Q, n_1) = 1, \; (N_1, n_1) = 1,$$

sodaß also 6) geschrieben werden kann:

$$x^{Qn_1} = \eta^{b_0} \quad (\mathfrak{p}).$$

Setzt man hierin $x^{n_1} = y$, so ergeben sich für die weitere Untersuchung die beiden Gleichungen:

9a) $$y^Q = \eta^{b_0} \quad (\mathfrak{p}),$$ 9b) $$x^{n_1} = y.$$

Die Zerlegung von $\mathfrak{p}$ in $k(x)$ führe ich in zwei Schritten aus, indem ich zuerst zeige, wie $\mathfrak{p}$ in dem durch Gleichung 9a) definierten Körper $k_y = k(y)$ in Primteiler $\overline{\mathfrak{P}}_i$ zerfällt, und dann wie jeder Primteiler $\overline{\mathfrak{P}}_i$ in dem durch Adjunktion einer Wurzel x der Gleichung 9b) zu k_y entstehenden Körper $k_y(x) = k(x)$ zerfällt.

Da Q nur aus in N_1 enthaltenen Primzahlen besteht und η^{b_0} eine primitive N_1-te Einheitswurzel ist, so folgt nach dem oben bewiesenen Hilfssatz (S. 35), daß jede Wurzel der Gleichung 9a) eine primitive QN_1-te Einheitswurzel ist. Ist y eine von ihnen, so genügt sie in $k(\mathfrak{p})$ nach dem auf S. 6 bewiesenen Hilfssatz 3 (den wir hier anwenden können, da $(p, QN_1) = 1$ ist, wie aus Q/n, $N_1/N/(p^f - 1)$ und der Voraussetzung $(p, n) = 1$ folgt) einer irreduziblen Gleichung vom Grade $f'^{(QN_1)}$, wenn $f'^{(QN_1)}$ der Exponent ist, zu dem p^f mod QN_1 gehört. Die Funktion $y^Q - \eta^{b_0}$ zerfällt daher

1) Dasselbe gilt in diesem Fall auch in dem von uns ausgeschlossenen Falle p/n, was genau so bewiesen wird.

in $k(\mathfrak{p})$ in $\frac{Q}{f'^{(QN_1)}}$ irreduzible Faktoren $f'^{(QN_1)}$-ten Grades, und jedem dieser Faktoren ist, wie aus dem Beweis von Satz 3 auf S. 7 hervorgeht, ein Primteiler $\bar{\mathfrak{P}}_i$ vom Relativgrade $f'^{(QN_1)}$ und der Relativordnung 1 bezügl. $\mathfrak{p}$ in k_y zuzuordnen. π bleibt daher auch Primelement in $k_y(\bar{\mathfrak{P}}_i)$. Für das Folgende bemerke ich noch, daß der Grad von $\bar{\mathfrak{P}}_i$ gleich $f'^{(QN_1)}$ ist.

Um nun weiter festzustellen, wie jeder dieser Primteiler $\bar{\mathfrak{P}}_i$ in $k(x)$ zerfällt, haben wir die Zerlegung von 9 b) im Bereiche $k_y(\bar{\mathfrak{P}}_i)$ zu untersuchen. Da y eine primitive QN_1-te Einheitswurzel in $k_y(\bar{\mathfrak{P}}_i)$ und $(n_1, QN_1) = 1$ ist, so kann man $\bar{n}_1$ so bestimmen, daß $\bar{n}_1 n_1 \equiv 1 \bmod QN_1$, also $y = (y^{\bar{n}_1})^{n_1} = y_0^{n_1}$ ist. y ist also n_1-ter Potenzrest bezügl. $\bar{\mathfrak{P}}_i$. Durch die Substitution $x' = \frac{x}{y_0}$ geht dann $x^{n_1} = y\ (\bar{\mathfrak{P}}_i)$ über in

$$10) \qquad x'^{n_1} = 1 \ . \ (\bar{\mathfrak{P}}_i),$$

und ich brauche jetzt nur noch zu untersuchen, wie diese Gleichung für den Bereich von $\bar{\mathfrak{P}}_i$ zerfällt. Sie besitzt nun schon im Körper $K(1)$ die Zerlegung $x'^{n_1} - 1 = \prod\limits_{m/n_1} F_m(x')$, wo m sämtliche Teiler von n_1 (inkl. 1 und n_1) durchläuft, und $F_m(x')$ den in $K(1)$ irreduziblen Faktor $\varphi(m)$-ten Grades von $x'^{n_1} - 1$ bedeutet, welcher nur die primitiven m-ten Einheitswurzeln enthält. Da wegen $m/n_1/n\ (p, m) = 1$ ist, so genügt nach Hilfssatz 3 (S. 6) jede primitive m-te Einheitswurzel einer irreduziblen Gleichung $f'^{(m)}$-ten Grades in $k_y(\bar{\mathfrak{P}}_i)$, wenn $p^{f'^{(QN_1)}}$ zum Exponenten $f'^{(m)}$ mod m gehört. $F_m(x')$ zerfällt also in $\frac{\varphi(m)}{f'^{(m)}}$ irreduzible Faktoren $f'^{(m)}$-ten Grades in $k_y(\bar{\mathfrak{P}}_i)$, und somit $x'^{n_1} - 1$ in $\sum\limits_{m/n_1} \frac{\varphi(m)}{f'^{(m)}}$ irreduzible Faktoren, von denen je $\frac{\varphi(m)}{f'^{(m)}}$ vom Grade $f'^{(m)}$ sind. Je $\frac{\varphi(m)}{f'^{(m)}}$ Faktoren ist ein Primteiler vom Relativgrade $f'^{(m)}$ bezügl. $\bar{\mathfrak{P}}_i$ und der Relativordnung 1 bezügl. $\bar{\mathfrak{P}}_i$ zuzuordnen, also vom Relativgrade $f'^{(QN_1)} f'^{(m)}$ bezügl. $\mathfrak{p}$ und der Relativordnung 1 bezügl. $\mathfrak{p}$. Insgesamt zerfällt daher $\mathfrak{p}$ in $k(x)$ in $\sigma = \frac{Q}{f'^{(QN_1)}} \sum\limits_{m/n_1} \frac{\varphi(m)}{f'^{(m)}}$ Primteiler, von denen je $\frac{Q}{f'^{(QN_1)}} \frac{\varphi(m)}{f'^{(m)}}$ vom Relativgrade $f'^{(QN_1)} f'^{(m)}$ und der Relativordnung 1 sind. Wir erhalten somit:

Satz 2. Ist $(a, n) = (a_0, n) = n$ $(a_0 = 0)$, $(b_0, p^f - 1, n^\infty) = \bar{b}$ und wird $(p^f - 1, n^\infty) = \bar{b} N_1$, $(n, N_1^\infty) = Q$ und $n = Q n_1$ gesetzt, so zerfällt $\mathfrak{p}$ in $k(x)$ in $\sigma = \frac{Q}{f'^{(QN_1)}} \sum_{m/n_1} \frac{\varphi(m)}{f'^{(m)}}$ Primteiler der Relativordnung 1, von denen je $\frac{Q}{f'^{(QN_1)}} \frac{\varphi(m)}{f'^{(m)}}$ vom Relativgrade $f'^{(QN_1)} f'^{(m)}$ sind, wobei die Summe in dem Ausdruck für σ über alle Teiler m von n_1 (incl. 1 und n_1) zu erstrecken ist, $f'^{(QN_1)}$ den Exponenten, zu dem p^f mod QN_1 und $f'^{(m)}$ den Exponenten, zu dem $p^{f'^{(QN_1)}}$ mod m gehört, bedeutet.

III. $$(a, n) = (a_0, n) = n' \gtrless \frac{1}{n}.$$

Dieser Fall läßt sich leicht mit Hilfe der Sätze 1 und 2 erledigen. Sei also:

11) $$(a_0, n) = n', \; a_0 = \bar{a} n', \; n = \bar{n} n'; \; (\bar{a}, \bar{n}) = 1.$$

Um das Ergebnis besser formulieren zu können, gehen wir nicht von der reduzierten Grundgleichung 4), sondern von der gleichbedeutenden Gleichung 2b)

$$x^n = \pi^{a_0} w^{b_0} \quad (\mathfrak{p})$$

aus (wo b_0 den kleinsten Rest von b mod n bedeutete). Sie kann jetzt geschrieben werden:

12) $$x^{\bar{n} n'} = \pi^{\bar{a} n'} w^{b_0} \quad (\mathfrak{p}).$$

Setzt man hierin $x^{\bar{n}} = y$, so ergeben sich aus 12) für die weitere Untersuchung die beiden Gleichungen:

13a) $$y^{n'} = \pi^{\bar{a} n'} w^{b_0} \quad (\mathfrak{p}) \qquad 13\,\text{b}) \; x^{\bar{n}} = y.$$

Durch die Substitution

14) $$\bar{y} = \frac{y}{\pi^{\bar{a}}}$$

kann 13a) reduziert werden auf

15) $$\bar{y}^{n'} = w^{b_0} \quad (\mathfrak{p}).$$

Wir setzen nun

16) $$(p^f - 1, \; n'^\infty) = N', \; p^f - 1 = N' P', \; w = \eta' \bar{\eta}' \quad (\mathfrak{p}),$$

wo η' eine primitive N'-te Einheitswurzel und $\bar{\eta}'$ eine primitive P'-te Einheitswurzel bedeutet, dann kann nach den früheren Prinzipien die Gleichung 15) auf die Form

17) $$y'^{n'} = \eta'^{b_0} \quad (\mathfrak{p})$$

gebracht werden, wo jetzt b_0 kleiner als die kleinere der beiden Zahlen n' und N' angenommen werden kann und soll. 17) stellt also in demselben Sinne die reduzierte Form der Gleichung $y^{n'} = A$ (p) dar wie 4) diejenige von $x^n = A$ (p). Auf 17) kann Satz 2 sinngemäß angewandt werden. Dies ergibt die Zerlegung von p in dem durch Gleichung 13a) definierten Körper $k(y) = k_y$. Ist $\overline{\mathfrak{P}}_i$ einer der Primteiler von p in k_y, von denen wir (nach Satz 2) wissen, daß ihre Relativordnung gleich 1 ist, so haben wir jetzt noch zu untersuchen, wie $\overline{\mathfrak{P}}_i$ in dem durch Gleichung 13b) definierten Oberkörper $k_y(x) = k(x)$ von $k(y)$ zerfällt, d. h. die Zerlegung der Funktion $x^{\bar{n}} - y$ in $k_y(\overline{\mathfrak{P}}_i)$ festzustellen. Nun ist aber nach 14) $y = \pi^{\bar{a}}\bar{y}$, wo $\bar{y}$ eine Einheit bezügl. $\overline{\mathfrak{P}}_i$ ist, weil $\bar{y}$ nach 15) eine Einheitswurzel ist. Da die Relativordnung von $\overline{\mathfrak{P}}_i$ bezügl. p gleich 1 ist, so ist π auch Primelement bezügl. $\overline{\mathfrak{P}}_i$, also $\bar{a}$ auch die Ordnungszahl von y bezügl. $\overline{\mathfrak{P}}_i$, und wegen $(\bar{a}, \bar{n}) = 1$ ist nach Satz 1 jedem $\overline{\mathfrak{P}}_i$ ein einziger Primteiler $\mathfrak{P}_i$ vom Relativgrade 1 und der Relativordnung $\bar{n} = \frac{n}{(a, n)}$ bezügl. $\overline{\mathfrak{P}}_i$ in $k_y(x) = k(x)$ zuzuordnen. Der Relativgrad von $\mathfrak{P}_i$ bezügl. p ist daher gleich dem Relativgrad von $\overline{\mathfrak{P}}_i$ bezügl. p und die Relativordnung von $\mathfrak{P}_i$ bezügl. p gleich $\frac{n}{(a, n)}$. Wir erhalten:

Satz 3. Im Falle $(a, n) = (a_0, n) = n' \gtrless_n^1$ zerfällt p in $k(x)$ in σ Primteiler von der Relativordnung $\frac{n}{(a, n)}$. Die Anzahl σ und der Relativgrad jedes einzelnen Primteilers sind aus der Gleichung 17) $y'^{n'} = \eta'^{b_0}$ (p), welches die reduzierte Form der Gleichung $y^{n'} = A$ (p) ist, zu bestimmen.

Dieser Satz enthält, wie man leicht sieht, die Sätze 1 und 2 als Sonderfälle in sich, wenn die Beschränkung $n' \gtrless_n^1$ fallen gelassen wird.

§ 3. Spezialfälle.

Sei zuerst die Grundzahl A n-ter Potenzrest bezügl. p, d. h. A_0 existiere in $k(\mathfrak{p})$, sodaß $A_0^n = A$ (p). Dies tritt (unter der von

uns gemachten Voraussetzung $(p, n) = 1$), wie Herr Hensel gezeigt hat, stets und nur dann ein, wenn die Ordnungszahl $a \equiv 0 \bmod n$ $(a_0 = 0)$, und der Index $b \equiv 0 \bmod (n, p^f - 1)$ ist[1]). Die letztere Bedingung ist dann stets, wie eine leichte Rechnung zeigt, auch für den reduzierten Index b_0 erfüllt. Die Grundgleichung $x^n = A$ kann durch die Substitution $x' = \frac{x}{A_0}$ auf die Form $x^n = 1$ (p) gebracht werden, und man erhält nach den früheren Prinzipien (Satz 2) sofort:

Satz 4. Ist A n-ter Potenzrest bezügl. p, so zerfällt p in $k(x)$ in $\sigma = \frac{\Sigma \varphi(m)}{m/n\, f'^{(m)}}$ Primteiler der Relativordnung 1, von denen je $\frac{\varphi(m)}{f'^{(m)}}$ vom Relativgrade $f'^{(m)}$ sind, wobei in der Summe m über alle Teiler von n zu erstrecken ist, und $f'^{(m)}$ den Exponenten bedeutet, zu dem $p^f \bmod m$ gehört.

Ein besonders einfaches Zerlegungsgesetz erhält man, wenn $k(\mathfrak{p})$ die primitiven n-ten Einheitswurzeln enthält, also $n/p^f - 1)$ ist (wegen $(p, n) = 1$), was sicher stets dann der Fall ist, wenn sie schon im Grundkörper k enthalten sind. Hier wird die Frage nach der Zerlegung von p durch folgenden Satz vollständig beantwortet.

Satz 5. Ist a die Ordnungszahl, b der Index von A bezügl. p und enthält $k(\mathfrak{p})$ die primitiven n-ten Einheitswurzeln, so zerfällt p in $k(x)$ in $\sigma = (a, b, n)$ verschiedene Primteiler vom Relativgrade $f_i' = \frac{(a, n)}{(a, b, n)}$ und der Relativordnung $e_i' = \frac{n}{(a, n)}$.

Speziell gilt dies also für die „allgemeinen“ Kummerschen Körper, wo $\mathfrak{K}_n$ der Grundkörper ist.

Der Beweis mit Hilfe der allgemeinen Sätze des vorhergehenden Paragraphen gestaltet sich etwas umständlich. Wir wollen daher einen einfacheren Weg einschlagen und diese nur zum Teil benutzen. Es folgt jedenfalls aus Satz 3 sofort, daß jeder Primteiler $\mathfrak{P}_i$ von p in $k(x)$ die Relativordnung $e_i' = \frac{n}{(a, n)}$ besitzt.

1) K. Hensel, „Die Verallgemeinerung des Legendreschen Symboles für allgemeine algebraische Körper“. Cr. J. 147 S. 242/3.

Es sei jetzt d der größte Teiler von n, für den A d-ter Potenzrest bezügl. $\mathfrak{p}$ ist, also A_0 in $k(\mathfrak{p})$ existiert, sodaß $A_0^d \equiv A\ (\mathfrak{p})$. d muß gleich (a, b, n) sein, denn damit A d-ter Potenzrest ist, muß nach der oben erwähnten notwendigen und hinreichenden Bedingung $a \equiv 0 \bmod d$, $b \equiv 0 \bmod (d, p^f - 1)$, also auch $b \equiv 0 \bmod d$ sein, weil $d/n/(p^f - 1)$, woraus nach der Bedeutung von d sich die Behauptung unmittelbar ergibt.

Bezeichnet nun ϱ eine primitive d-te Einheitswurzel, welche wegen d/n in $k(\mathfrak{p})$ enthalten ist, so kann die Grundgleichung $x^n \equiv A\ (\mathfrak{p})$ sofort zerlegt werden in:

$$18) \qquad x^n - A = \prod_{i=0}^{d-1} (x^{\frac{n}{d}} - A_0 \varrho^i)\ (\mathfrak{p}) \qquad (d = (a, b, n)).$$

Diese Faktoren sind, wie ich gleich zeigen werde, irreduzibel in $k(\mathfrak{p})$. Daraus folgt aber dann sofort Satz 5. Denn ordnet man jedem der Faktoren $x^{\frac{n}{d}} - A_0 \varrho^i$ einen Primteiler $\mathfrak{P}_i$ von $\mathfrak{p}$ vom Relativgrade f_i' und der Relativordnung e_i' zu, so ergibt sich ja aus

$$e_i' f_i' = \frac{n}{d} = \frac{n}{(a, b, n)} \quad \text{und} \quad e_i' = \frac{n}{(a, n)},$$

daß

$$f_i' = \frac{(a, n)}{(a, b, n)}$$

ist, wie in Satz 5 behauptet wurde.

Es ist jetzt nur noch die Irreduktibilität der Faktoren $x^{\frac{n}{d}} - A_0 \varrho^i$ in $k(\mathfrak{p})$ zu zeigen. Wir nehmen nun an, $x^{\frac{n}{d}} - A_0 \varrho^i$ wäre reduzibel, $h(x)$ sei einer seiner irreduziblen Faktoren in $k(\mathfrak{p})$ und v der Grad von $h(x)$ $\left(v < \frac{n}{d}\right)$. Da $h(x)/(x^{\frac{n}{d}} - A_0 \varrho^i)/(x^n - A)$, so haben die Wurzeln von $h(x)$ die Form

$$x_0 \omega^{i_1},\ x_0 \omega^{i_2},\ \ldots\ x_0 \omega^{i_v},$$

wo x_0 irgendeine Wurzel von $x^n - A \equiv 0\ (\mathfrak{p})$ und ω eine primitive n-te Einheitswurzel bedeutet. Nun ist aber das Produkt aller dieser Wurzeln als elementar-symmetrische Funktion aller Wurzeln von $h(x)$ eine Zahl aus $k(\mathfrak{p})$. Also:

$$x_0^v \omega^{\Sigma i_l} = \alpha \qquad \text{Zahl aus } k(\mathfrak{p}),$$

$$x_0^{v} \quad = \frac{\alpha}{\omega^{\Sigma i_l}} = \beta \quad \text{„} \quad \text{„} \quad \text{„} \ .$$

Sei nun $\left(v, \frac{n}{d}\right) = v_0$ und $\frac{n}{d} = v_0 c$ $\left(c > 1, \text{ weil } v < \frac{n}{d}\right)$, dann können wir zwei ganze Zahlen r_1 und r_2 so bestimmen, daß

$$v_0 = v r_1 + \frac{n}{d} r_2,$$

also

$$x_0^{v_0} = x_0^{v r_1 + \frac{n}{d} r_2} = \beta^{r_1} (A_0 \varrho^{i})^{r_2} = \gamma \text{ Zahl aus } k(\mathfrak{p}).$$

Hieraus folgt $A = x_0^n = \left(x_0^{\frac{n}{d}}\right)^d = (x_0^{v_0 c})^d = \gamma^{cd}$ $(\mathfrak{p})$, d. h. A wäre cd-ter Potenzrest bezügl. $\mathfrak{p}$ $(c > 1)$, was nach der Bedeutung von d unmöglich ist, also muß $x^{\frac{n}{d}} - A_0 \varrho^i$ irreduzibel sein.

Anhang.

Ueber algebraische Auflösbarkeit Galoisscher Polynome.

Es sei $F(x)$ ein Galoissches Polynom über $K(1)$ vom Grade m [1]). Ich will zunächst folgenden Satz beweisen:

Satz 1. $F(x)$ ist sicher dann algebraisch auflösbar (über $K(1)$), wenn eine Primzahl p existiert, sodaß $F(x)$ auch irreduzibel in $K(p)$ ist.

Ist nämlich $\bar{W}$ der Wurzelkörper von $F(x)$ über $K(p)$, so ist nach einem allgemeinen von Herrn Hensel herrührenden Theorem $\bar{W}$ sicher ein auflösbarer Körper über $K(p)$ [2]), d. h. die Galoissche Gruppe G von $\bar{W}$ bezügl. $K(p)$ ist metazyklisch. Ist nun $F(x)$ auch irreduzibel in $K(p)$, und bedeutet W den Wurzelkörper von $F(x)$ über $K(1)$, so ist G auch die Galoissche Gruppe von W bezügl. $K(1)$, da ja dann $\bar{W}$ über $K(p)$ und W über $K(1)$ vom selben Grade sind und, wenn α eine Wurzel von $F(x)$ 0, α sowohl primitives Element von W als auch von $\bar{W}$ ist, also die Galoissche Gruppe von $\bar{W}$ bezügl. $K(p)$ bzw. von W bezügl. $K(1)$ durch die Gruppe der Substitutionen $(\alpha \to \alpha_1, \alpha \to \alpha_2, \ldots \alpha \to \alpha_m)$, wo $\alpha_1, \alpha_2, \ldots \alpha_m$ sämtliche Wurzeln von $F(x)$ sind, dargestellt werden kann, womit alles bewiesen ist.

Als einfache Anwendung erwähne ich, daß hieraus die algebraische Auflösbarkeit der Kreisteilungsgleichung folgt. Denn wir hatten ja gesehen, daß die Gleichung der primitiven p^h-ten

1) d. h. ein in $K(1)$ irreduzibles Polynom, dessen sämtliche Wurzeln sich rational mit Koeffizienten aus $K(1)$ durch eine von ihnen darstellen lassen.

2) M. Z. 2 S. 451.

Einheitswurzeln (p Primzahl), welche ja eine Galoissche Gleichung über $K(1)$ ist, in $K(p)$ irreduzibel ist. Weiter ergibt sich aus dem Satze, daß auch jedes Galoissche-Eisensteinsche Polynom über $K(1)$ $F(x) = x^m + pa_1x^{m-1} + \ldots + pa_m$, dessen konstantes Glied die Primzahl p nur in der ersten Potenz enthält, algebraisch auflösbar ist, weil ja auch es in $K(p)$ irreduzibel ist. Als zahlentheoretische Folgerung aus Satz 1 ergibt sich, daß in einem Galoisschen algebraischen Zahlkörper N, welcher nicht über $K(1)$ algebraisch auflösbar ist, sämtliche Primzahlen in verschiedene (also mindestens 2) Primideale zerfallen, denn sonst müßte ja das N definierende Galoissche Polynom $F(x)$ aus $K(1)$ für den Bereich mindestens einer Primzahl irreduzibel, N also entgegen der Annahme auflösbar sein.

Ob das in Satz 1 angegebene Kriterium auch notwendig ist, will ich in einer späteren Arbeit untersuchen. Ist dies der Fall, dann würde hieraus folgen, daß dann und nur dann, wenn N ein über $K(1)$ auflösbarer Galoisscher algebraischer Zahlkörper ist, es Primzahlen gibt, die in ihm nicht in verschiedene Primideale zerfallen.

Es sei jetzt wieder wie vorhin W der Wurzelkörper irgend eines Galoisschen Polynoms $F(x)$ über $K(1)$, dann gilt folgender Satz:

Satz 2. *W enthält stets einen echten Unterkörper Z, über dem $F(x)$ algebraisch auflösbar ist.*

Sei nämlich

$$F(x) \equiv f_1(x) f_2(x) \ldots f_r(x) \quad (p)$$

die Zerlegung von $F(x)$ in $K(p)$, wo p eine beliebige Primzahl ist. Da $F(x)$ Galoissch ist, so sind alle Faktoren $f_i(x)$ vom gleichen Grade r und ebenfalls Galoissch. Daher ist W_r der Wurzelkörper von $F(x)$ über $K(p)$, vom r-ten Grade über $K(p)$. Ist $f(x)$ irgend einer der Faktoren von $F(x)$, α eine Wurzel der Gleichung $f(x) \equiv 0 \ (p)$, so ist α ein primitives Element von W_r und $\mathfrak{G}(\alpha \to \alpha_1, \alpha \to \alpha_2, \ldots \alpha \to \alpha_r)$, wo $\alpha_1, \alpha_2, \ldots \alpha_r$ sämtliche Wurzeln von $f(x)$ sind, die Galoissche Gruppe von W_r bezügl. $K(p)$ bezw. von $f(x)$ bezügl. $K(p)$. Sie ist nach dem oben erwähnten allgemeinen Theorem metazyklisch und eine Untergruppe der Galoisschen Gruppe von $F(x)$ bezügl. $K(1)$. Der zu ihr gehörige Unterkörper von W werde mit Z bezeichnet, dann ist also $\mathfrak{G}(\alpha \to \alpha_i)$ die Galoissche Gruppe von W bezügl. Z

und daher W über Z algebraisch auflösbar. Da, wenn p Diskriminantenteiler, sicher r größer als 1 ist, so ist der Satz bewiesen. $\overline{\mathfrak{G}}\,(\bar{\alpha} \to \bar{\alpha}_i)$ ist nichts anderes als die Zerlegungsgruppe des $f(x)$ zugeordneten Primteilers von p und Z der Zerlegungs-Körper[1]). Wir können den Satz 2 daher auch so aussprechen: Jeder Galoissche algebraische Zahlkörper ist über den zu seinen Primteilern gehörigen Zerlegungskörpern algebraisch auflösbar, welches Resultat schon von Herrn Hilbert bewiesen wurde[2]).

---

1) Vgl. F. Hüttig, „Arithmetische Theorie eines Galoisschen Körpers". Marb. Phil. Diss. 1907.

2) D. Hilbert, „Die Theorie der algebraischen Zahlkörper". Jahresber. d. deutschen Math. Ver. Bd. 4 § 49 Satz 82.

Lebenslauf.

Ich, Michael Friedrich Oppenheimer, wurde am 18. April 1904 als Sohn des Kaufmanns Heinrich Oppenheimer und seiner Ehefrau Elise geb. Strauß zu Michelstadt i. Odenwald geboren. Ich bin hessischer Staatsangehörigkeit und israelitischer Konfession. Nach einjährigem Besuch der Volksschule trat ich in die Vorschule der Realschule über und besuchte von Ostern 1913 bis Ostern 1920 die Realschule zu Michelstadt. Das Reifezeugnis erhielt ich Ostern 1922 am Hess. Realgymnasium zu Darmstadt. Seitdem studierte ich Mathematik, Physik und Philosophie an den Universitäten Frankfurt a. Main (S.-S. 1922 bis W.-S. 1923/24), Marburg a. d. Lahn (S.-S. 1924 bis W.-S. 1924/25 und W.-S. 1925/26 bis jetzt) und Hamburg (S.-S. 1925). In den beiden ersten Semestern widmete ich mich gleichzeitig eingehenderen talmudischen Studien an der Thoralehranstalt des Herrn Rabbiner Dr. S. Breuer s. A. zu Frankfurt a. Main.

Das Rigorosum bestand ich am 17. Juli 1929.

Meine akademischen Lehrer waren die Herren Professoren und Dozenten:

v. Braun, Brendel, Cornelius, Dehn, Hasse, Heinemann, Hellinger, M. E. Mayer †, v. Petzold, Siegel, Schultz, Schulz-Schaeffer und Wachsmuth in Frankfurt,

Artin, Blaschke, Cassirer, Goos und Schreier in Hamburg,

Berek, Fraenkel, Grüneisen, Hartmann, Heidegger, Hensel, Hölscher, Jaeck, Jaensch, Lange, Neumann, Otto, Rehmke, Schaefer, F. A. Schulze, Senftleben, Thiel, Tomaschek und Zühlke in Marburg.

Allen meinen sehr verehrten Lehrern bin ich zu wärmstem Dank verpflichtet, namentlich aber Herrn Geh. Reg.-Rat Prof. Dr. K. Hensel, der die Anregung zu der vorliegenden Arbeit gab und ihrer Ausführung stets reiches Interesse entgegenbrachte.